Referenzhandbuch

AWS Verwaltete Richtlinie

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Verwaltete Richtlinie: Referenzhandbuch

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was sind AWS verwaltete Richtlinien? 1
Referenzseiten zu Richtlinien verstehen 1
Veraltete verwaltete Richtlinien AWS 2
AWS verwaltete Richtlinien 3
AccessAnalyzerServiceRolePolicy 52
Diese Richtlinie wird verwendet 52
Einzelheiten der Richtlinie 52
Version der Richtlinie 52
JSON-Richtliniendokument 53
Weitere Informationen 55
AccountManagementFromVercel 55
Diese Richtlinie wird verwendet 56
Einzelheiten zur Richtlinie 56
Version der Richtlinie 56
JSON-Richtliniendokument 56
Weitere Informationen 57
AdministratorAccess 57
Diese Richtlinie wird verwendet 57
Einzelheiten zur Richtlinie 57
Version der Richtlinie 58
JSON-Richtliniendokument 58
Weitere Informationen 58
AdministratorAccess-Amplify 58
Diese Richtlinie wird verwendet 59
Einzelheiten zur Richtlinie 59
Version der Richtlinie 59
JSON-Richtliniendokument 59
Weitere Informationen 69
AdministratorAccess-AWSElasticBeanstalk 70
Diese Richtlinie wird verwendet 70
Einzelheiten zur Richtlinie 70
Version der Richtlinie 70
JSON-Richtliniendokument 70
Weitere Informationen 79

AIOpsAssistantIncidentReportPolicy 79
Diese Richtlinie wird verwendet 79
Einzelheiten zur Richtlinie 79
Version der Richtlinie 79
JSON-Richtliniendokument 80
Weitere Informationen 80
AIOpsAssistantPolicy 81
Diese Richtlinie wird verwendet 81
Einzelheiten zur Richtlinie 81
Version der Richtlinie 81
JSON-Richtliniendokument 81
Weitere Informationen 102
AIOpsConsoleAdminPolicy 102
Diese Richtlinie wird verwendet 102
Einzelheiten zur Richtlinie 102
Version der Richtlinie 103
JSON-Richtliniendokument 103
Weitere Informationen 109
AIOpsOperatorAccess 109
Diese Richtlinie wird verwendet 109
Einzelheiten zur Richtlinie 109
Version der Richtlinie 110
JSON-Richtliniendokument 110
Weitere Informationen 113
AIOpsReadOnlyAccess 113
Diese Richtlinie wird verwendet 113
Einzelheiten zur Richtlinie 113
Version der Richtlinie 113
JSON-Richtliniendokument 114
Weitere Informationen 114
AlexaForBusinessDeviceSetup 114
Diese Richtlinie wird verwendet 115
Einzelheiten zur Richtlinie 115
Version der Richtlinie 115
JSON-Richtliniendokument 115
Weitere Informationen 116

AlexaForBusinessFullAccess 116
Diese Richtlinie wird verwendet 116
Einzelheiten zur Richtlinie 116
Version der Richtlinie 117
JSON-Richtliniendokument 117
Weitere Informationen 118
AlexaForBusinessGatewayExecution 118
Diese Richtlinie wird verwendet 119
Einzelheiten zur Richtlinie 119
Version der Richtlinie 119
JSON-Richtliniendokument 119
Weitere Informationen 120
AlexaForBusinessLifesizeDelegatedAccessPolicy 120
Diese Richtlinie wird verwendet 120
Einzelheiten zur Richtlinie 121
Version der Richtlinie 121
JSON-Richtliniendokument 121
Weitere Informationen 123
AlexaForBusinessNetworkProfileServicePolicy 124
Diese Richtlinie wird verwendet 124
Einzelheiten der Richtlinie 124
Version der Richtlinie 124
JSON-Richtliniendokument 124
Weitere Informationen 125
AlexaForBusinessPolyDelegatedAccessPolicy 125
Diese Richtlinie wird verwendet 125
Einzelheiten zur Richtlinie 126
Version der Richtlinie 126
JSON-Richtliniendokument 126
Weitere Informationen 128
AlexaForBusinessReadOnlyAccess 128
Diese Richtlinie wird verwendet 128
Einzelheiten zur Richtlinie 128
Version der Richtlinie 128
JSON-Richtliniendokument 129
Weitere Informationen 129

AmazonAPIGatewayAdministrator 129
Diese Richtlinie wird verwendet 129
Einzelheiten zur Richtlinie 130
Version der Richtlinie 130
JSON-Richtliniendokument 130
Weitere Informationen 130
AmazonAPIGatewayInvokeFullAccess 131
Diese Richtlinie wird verwendet 131
Einzelheiten zur Richtlinie 131
Version der Richtlinie 131
JSON-Richtliniendokument 131
Weitere Informationen 132
AmazonAPIGatewayPushToCloudWatchLogs 132
Diese Richtlinie wird verwendet 132
Einzelheiten zur Richtlinie 132
Version der Richtlinie 132
JSON-Richtliniendokument 133
Weitere Informationen 133
AmazonAppFlowFullAccess 133
Diese Richtlinie wird verwendet 134
Einzelheiten zur Richtlinie 134
Version der Richtlinie 134
JSON-Richtliniendokument 134
Weitere Informationen 137
AmazonAppFlowReadOnlyAccess 137
Diese Richtlinie wird verwendet 137
Einzelheiten zur Richtlinie 137
Version der Richtlinie 138
JSON-Richtliniendokument 138
Weitere Informationen 138
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 139
Diese Richtlinie wird verwendet 139
Einzelheiten zur Richtlinie 139
Version der Richtlinie 139
JSON-Richtliniendokument 139
Weitere Informationen 140

AmazonAppStreamFullAccess 140
Diese Richtlinie wird verwendet 141
Einzelheiten zur Richtlinie 141
Version der Richtlinie 141
JSON-Richtliniendokument 141
Weitere Informationen 143
AmazonAppStreamPCAAccess 143
Diese Richtlinie wird verwendet 143
Einzelheiten zur Richtlinie 143
Version der Richtlinie 144
JSON-Richtliniendokument 144
Weitere Informationen 144
AmazonAppStreamReadOnlyAccess 145
Diese Richtlinie wird verwendet 145
Einzelheiten zur Richtlinie 145
Version der Richtlinie 145
JSON-Richtliniendokument 145
Weitere Informationen 146
AmazonAppStreamServiceAccess 146
Diese Richtlinie wird verwendet 146
Einzelheiten zur Richtlinie 146
Version der Richtlinie 146
JSON-Richtliniendokument 147
Weitere Informationen 148
AmazonAthenaFullAccess 148
Diese Richtlinie wird verwendet 148
Einzelheiten zur Richtlinie 148
Version der Richtlinie 148
JSON-Richtliniendokument 149
Weitere Informationen 152
AmazonAthenaServiceRolePolicy 152
Diese Richtlinie wird verwendet 153
Einzelheiten der Richtlinie 153
Version der Richtlinie 153
JSON-Richtliniendokument 153
Weitere Informationen 154

AmazonAugmentedAIFullAccess 154
Diese Richtlinie wird verwendet 154
Einzelheiten zur Richtlinie 154
Version der Richtlinie 154
JSON-Richtliniendokument 155
Weitere Informationen 156
AmazonAugmentedAIHumanLoopFullAccess 156
Diese Richtlinie wird verwendet 156
Einzelheiten zur Richtlinie 156
Version der Richtlinie 156
JSON-Richtliniendokument 157
Weitere Informationen 157
AmazonAugmentedAIIntegratedAPIAccess 157
Diese Richtlinie wird verwendet 157
Einzelheiten zur Richtlinie 158
Version der Richtlinie 158
JSON-Richtliniendokument 158
Weitere Informationen 159
AmazonAuroraDSQLConsoleFullAccess 160
Diese Richtlinie wird verwendet 160
Einzelheiten zur Richtlinie 160
Version der Richtlinie 160
JSON-Richtliniendokument 160
Weitere Informationen 162
AmazonAuroraDSQLFullAccess 163
Diese Richtlinie wird verwendet 163
Einzelheiten zur Richtlinie 163
Version der Richtlinie 163
JSON-Richtliniendokument 163
Weitere Informationen 165
AmazonAuroraDSQLReadOnlyAccess 166
Diese Richtlinie wird verwendet 166
Einzelheiten zur Richtlinie 166
Version der Richtlinie 166
JSON-Richtliniendokument 166
Weitere Informationen 167

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy 167
Diese Richtlinie wird verwendet 168
Einzelheiten zur Richtlinie 168
Version der Richtlinie 168
JSON-Richtliniendokument 168
Weitere Informationen 169
AmazonBedrockFullAccess 169
Diese Richtlinie wird verwendet 169
Einzelheiten zur Richtlinie 169
Version der Richtlinie 169
JSON-Richtliniendokument 170
Weitere Informationen 175
AmazonBedrockLimitedAccess 175
Diese Richtlinie wird verwendet 175
Einzelheiten zur Richtlinie 175
Version der Richtlinie 176
JSON-Richtliniendokument 176
Weitere Informationen 178
AmazonBedrockMantleFullAccess 178
Diese Richtlinie wird verwendet 178
Einzelheiten zur Richtlinie 178
Version der Richtlinie 179
JSON-Richtliniendokument 179
Weitere Informationen 179
AmazonBedrockMantleInferenceAccess 179
Diese Richtlinie wird verwendet 180
Einzelheiten zur Richtlinie 180
Version der Richtlinie 180
JSON-Richtliniendokument 180
Weitere Informationen 181
AmazonBedrockMantleReadOnly 181
Diese Richtlinie wird verwendet 181
Einzelheiten zur Richtlinie 181
Version der Richtlinie 181
JSON-Richtliniendokument 182
Weitere Informationen 182

AmazonBedrockMarketplaceAccess 183
Diese Richtlinie wird verwendet 183
Einzelheiten zur Richtlinie 183
Version der Richtlinie 183
JSON-Richtliniendokument 183
Weitere Informationen 188
AmazonBedrockReadOnly 188
Diese Richtlinie wird verwendet 188
Einzelheiten zur Richtlinie 188
Version der Richtlinie 188
JSON-Richtliniendokument 188
Weitere Informationen 190
AmazonBedrockStudioPermissionsBoundary 190
Diese Richtlinie wird verwendet 190
Einzelheiten zur Richtlinie 190
Version der Richtlinie 191
JSON-Richtliniendokument 191
Weitere Informationen 195
AmazonBraketFullAccess 195
Diese Richtlinie wird verwendet 195
Einzelheiten zur Richtlinie 195
Version der Richtlinie 196
JSON-Richtliniendokument 196
Weitere Informationen 200
AmazonBraketJobsExecutionPolicy 200
Diese Richtlinie wird verwendet 200
Einzelheiten zur Richtlinie 200
Version der Richtlinie 201
JSON-Richtliniendokument 201
Weitere Informationen 203
AmazonBraketServiceRolePolicy 204
Diese Richtlinie wird verwendet 204
Einzelheiten der Richtlinie 204
Version der Richtlinie 204
JSON-Richtliniendokument 204
Weitere Informationen 205

AmazonChimeFullAccess 206
Diese Richtlinie wird verwendet 206
Einzelheiten zur Richtlinie 206
Version der Richtlinie 206
JSON-Richtliniendokument 206
Weitere Informationen 208
AmazonChimeReadOnly 209
Diese Richtlinie wird verwendet 209
Einzelheiten zur Richtlinie 209
Version der Richtlinie 209
JSON-Richtliniendokument 209
Weitere Informationen 210
AmazonChimeSDK 210
Diese Richtlinie wird verwendet 210
Einzelheiten zur Richtlinie 210
Version der Richtlinie 210
JSON-Richtliniendokument 211
Weitere Informationen 212
AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy 212
Diese Richtlinie wird verwendet 212
Einzelheiten der Richtlinie 212
Version der Richtlinie 212
JSON-Richtliniendokument 213
Weitere Informationen 214
AmazonChimeSDKMessagingServiceRolePolicy 214
Diese Richtlinie wird verwendet 214
Einzelheiten der Richtlinie 214
Version der Richtlinie 215
JSON-Richtliniendokument 215
Weitere Informationen 216
AmazonChimeServiceRolePolicy 216
Diese Richtlinie wird verwendet 216
Einzelheiten der Richtlinie 216
Version der Richtlinie 216
JSON-Richtliniendokument 217
Weitere Informationen 217

AmazonChimeTranscriptionServiceLinkedRolePolicy 217
Diese Richtlinie wird verwendet 218
Einzelheiten der Richtlinie 218
Version der Richtlinie 218
JSON-Richtliniendokument 218
Weitere Informationen 219
AmazonChimeUserManagement 219
Diese Richtlinie wird verwendet 219
Einzelheiten zur Richtlinie 219
Version der Richtlinie 219
JSON-Richtliniendokument 219
Weitere Informationen 221
AmazonChimeVoiceConnectorServiceLinkedRolePolicy 221
Diese Richtlinie wird verwendet 221
Einzelheiten der Richtlinie 221
Version der Richtlinie 221
JSON-Richtliniendokument 222
Weitere Informationen 223
AmazonCloudDirectoryFullAccess 224
Diese Richtlinie wird verwendet 224
Einzelheiten zur Richtlinie 224
Version der Richtlinie 224
JSON-Richtliniendokument 224
Weitere Informationen 225
AmazonCloudDirectoryReadOnlyAccess 225
Diese Richtlinie wird verwendet 225
Einzelheiten zur Richtlinie 225
Version der Richtlinie 225
JSON-Richtliniendokument 226
Weitere Informationen 226
AmazonCloudWatchEvidentlyFullAccess 226
Diese Richtlinie wird verwendet 226
Einzelheiten zur Richtlinie 227
Version der Richtlinie 227
JSON-Richtliniendokument 227
Weitere Informationen 229

AmazonCloudWatchEvidentlyReadOnlyAccess 230
Diese Richtlinie wird verwendet 230
Einzelheiten zur Richtlinie 230
Version der Richtlinie 230
JSON-Richtliniendokument 230
Weitere Informationen 231
AmazonCloudWatchEvidentlyServiceRolePolicy 231
Diese Richtlinie wird verwendet 231
Einzelheiten der Richtlinie 231
Version der Richtlinie 232
JSON-Richtliniendokument 232
Weitere Informationen 233
AmazonCloudWatchRUMFullAccess 234
Diese Richtlinie wird verwendet 234
Einzelheiten zur Richtlinie 234
Version der Richtlinie 234
JSON-Richtliniendokument 234
Weitere Informationen 237
AmazonCloudWatchRUMReadOnlyAccess 237
Diese Richtlinie wird verwendet 237
Einzelheiten zur Richtlinie 237
Version der Richtlinie 237
JSON-Richtliniendokument 238
Weitere Informationen 239
AmazonCloudWatchRUMServiceRolePolicy 239
Diese Richtlinie wird verwendet 239
Einzelheiten der Richtlinie 240
Version der Richtlinie 240
JSON-Richtliniendokument 240
Weitere Informationen 241
AmazonCodeCatalystFullAccess 241
Diese Richtlinie wird verwendet 241
Einzelheiten zur Richtlinie 241
Version der Richtlinie 241
JSON-Richtliniendokument 242
Weitere Informationen 242

AmazonCodeCatalystReadOnlyAccess 243
Diese Richtlinie wird verwendet 243
Einzelheiten zur Richtlinie 243
Version der Richtlinie 243
JSON-Richtliniendokument 243
Weitere Informationen 244
AmazonCodeCatalystSupportAccess 244
Diese Richtlinie wird verwendet 244
Einzelheiten zur Richtlinie 244
Version der Richtlinie 244
JSON-Richtliniendokument 245
Weitere Informationen 245
AmazonCodeGuruProfilerAgentAccess 246
Diese Richtlinie wird verwendet 246
Einzelheiten zur Richtlinie 246
Version der Richtlinie 246
JSON-Richtliniendokument 246
Weitere Informationen 247
AmazonCodeGuruProfilerFullAccess 247
Diese Richtlinie wird verwendet 247
Einzelheiten zur Richtlinie 247
Version der Richtlinie 247
JSON-Richtliniendokument 248
Weitere Informationen 248
AmazonCodeGuruProfilerReadOnlyAccess 249
Diese Richtlinie wird verwendet 249
Einzelheiten zur Richtlinie 249
Version der Richtlinie 249
JSON-Richtliniendokument 249
Weitere Informationen 250
AmazonCodeGuruReviewerFullAccess 250
Diese Richtlinie wird verwendet 250
Einzelheiten zur Richtlinie 250
Version der Richtlinie 251
JSON-Richtliniendokument 251
Weitere Informationen 253

AmazonCodeGuruReviewerReadOnlyAccess 254
Diese Richtlinie wird verwendet 254
Einzelheiten zur Richtlinie 254
Version der Richtlinie 254
JSON-Richtliniendokument 254
Weitere Informationen 255
AmazonCodeGuruReviewerServiceRolePolicy 255
Diese Richtlinie wird verwendet 255
Einzelheiten der Richtlinie 255
Version der Richtlinie 256
JSON-Richtliniendokument 256
Weitere Informationen 258
AmazonCodeGuruSecurityFullAccess 258
Diese Richtlinie wird verwendet 258
Einzelheiten zur Richtlinie 258
Version der Richtlinie 258
JSON-Richtliniendokument 259
Weitere Informationen 259
AmazonCodeGuruSecurityScanAccess 259
Diese Richtlinie wird verwendet 259
Einzelheiten zur Richtlinie 259
Version der Richtlinie 260
JSON-Richtliniendokument 260
Weitere Informationen 260
AmazonCognitoDeveloperAuthenticatedIdentities 261
Diese Richtlinie wird verwendet 261
Einzelheiten zur Richtlinie 261
Version der Richtlinie 261
JSON-Richtliniendokument 261
Weitere Informationen 262
AmazonCognitoIdpEmailServiceRolePolicy 262
Diese Richtlinie wird verwendet 262
Einzelheiten der Richtlinie 262
Version der Richtlinie 263
JSON-Richtliniendokument 263
Weitere Informationen 263

AmazonCognitoIdpServiceRolePolicy 264
Diese Richtlinie wird verwendet 264
Einzelheiten der Richtlinie 264
Version der Richtlinie 264
JSON-Richtliniendokument 264
Weitere Informationen 265
AmazonCognitoPowerUser 265
Diese Richtlinie wird verwendet 265
Einzelheiten zur Richtlinie 265
Version der Richtlinie 265
JSON-Richtliniendokument 266
Weitere Informationen 267
AmazonCognitoReadOnly 267
Diese Richtlinie wird verwendet 267
Einzelheiten zur Richtlinie 267
Version der Richtlinie 268
JSON-Richtliniendokument 268
Weitere Informationen 269
AmazonCognitoUnAuthedIdentitiesSessionPolicy 269
Diese Richtlinie wird verwendet 269
Einzelheiten zur Richtlinie 269
Version der Richtlinie 270
JSON-Richtliniendokument 270
Weitere Informationen 271
AmazonCognitoUnauthenticatedIdentities 271
Diese Richtlinie wird verwendet 271
Einzelheiten zur Richtlinie 271
Version der Richtlinie 272
JSON-Richtliniendokument 272
Weitere Informationen 272
AmazonConnect_FullAccess 272
Diese Richtlinie wird verwendet 273
Einzelheiten zur Richtlinie 273
Version der Richtlinie 273
JSON-Richtliniendokument 273
Weitere Informationen 276

AmazonConnectCampaignsServiceLinkedRolePolicy 276
Diese Richtlinie wird verwendet 276
Einzelheiten der Richtlinie 276
Version der Richtlinie 276
JSON-Richtliniendokument 277
Weitere Informationen 279
AmazonConnectReadOnlyAccess 279
Diese Richtlinie wird verwendet 279
Einzelheiten zur Richtlinie 279
Version der Richtlinie 279
JSON-Richtliniendokument 279
Weitere Informationen 280
AmazonConnectServiceLinkedRolePolicy 280
Diese Richtlinie wird verwendet 281
Einzelheiten der Richtlinie 281
Version der Richtlinie 281
JSON-Richtliniendokument 281
Weitere Informationen 294
AmazonConnectSynchronizationServiceRolePolicy 294
Diese Richtlinie wird verwendet 294
Einzelheiten der Richtlinie 294
Version der Richtlinie 294
JSON-Richtliniendokument 295
Weitere Informationen 297
AmazonConnectVoiceIDFullAccess 297
Diese Richtlinie wird verwendet 297
Einzelheiten zur Richtlinie 297
Version der Richtlinie 297
JSON-Richtliniendokument 297
Weitere Informationen 298
AmazonDataZoneBedrockModelConsumptionPolicy 298
Diese Richtlinie wird verwendet 298
Einzelheiten zur Richtlinie 298
Version der Richtlinie 299
JSON-Richtliniendokument 299
Weitere Informationen 301

AmazonDataZoneBedrockModelManagementPolicy 301
Diese Richtlinie wird verwendet 302
Einzelheiten zur Richtlinie 302
Version der Richtlinie 302
JSON-Richtliniendokument 302
Weitere Informationen 304
AmazonDataZoneDomainExecutionRolePolicy 304
Diese Richtlinie wird verwendet 304
Einzelheiten zur Richtlinie 304
Version der Richtlinie 305
JSON-Richtliniendokument 305
Weitere Informationen 308
AmazonDataZoneEnvironmentRolePermissionsBoundary 309
Diese Richtlinie wird verwendet 309
Einzelheiten zur Richtlinie 309
Version der Richtlinie 309
JSON-Richtliniendokument 309
Weitere Informationen 322
AmazonDataZoneFullAccess 322
Diese Richtlinie wird verwendet 323
Einzelheiten zur Richtlinie 323
Version der Richtlinie 323
JSON-Richtliniendokument 323
Weitere Informationen 332
AmazonDataZoneFullUserAccess 332
Diese Richtlinie wird verwendet 332
Einzelheiten zur Richtlinie 333
Version der Richtlinie 333
JSON-Richtliniendokument 333
Weitere Informationen 336
AmazonDataZoneGlueManageAccessRolePolicy 337
Diese Richtlinie wird verwendet 337
Einzelheiten zur Richtlinie 337
Version der Richtlinie 337
JSON-Richtliniendokument 337
Weitere Informationen 345

AmazonDataZonePortalFullAccessPolicy 345
Diese Richtlinie wird verwendet 346
Einzelheiten zur Richtlinie 346
Version der Richtlinie 346
JSON-Richtliniendokument 346
Weitere Informationen 346
AmazonDataZonePreviewConsoleFullAccess 347
Diese Richtlinie wird verwendet 347
Einzelheiten zur Richtlinie 347
Version der Richtlinie 347
JSON-Richtliniendokument 347
Weitere Informationen 349
AmazonDataZoneProjectDeploymentPermissionsBoundary 350
Diese Richtlinie wird verwendet 350
Einzelheiten zur Richtlinie 350
Version der Richtlinie 350
JSON-Richtliniendokument 350
Weitere Informationen 358
AmazonDataZoneProjectRolePermissionsBoundary 359
Diese Richtlinie wird verwendet 359
Einzelheiten zur Richtlinie 359
Version der Richtlinie 359
JSON-Richtliniendokument 359
Weitere Informationen 366
AmazonDataZoneRedshiftGlueProvisioningPolicy 367
Diese Richtlinie wird verwendet 367
Einzelheiten zur Richtlinie 367
Version der Richtlinie 367
JSON-Richtliniendokument 368
Weitere Informationen 375
AmazonDataZoneRedshiftManageAccessRolePolicy 375
Diese Richtlinie wird verwendet 376
Einzelheiten zur Richtlinie 376
Version der Richtlinie 376
JSON-Richtliniendokument 376
Weitere Informationen 379

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 380
Diese Richtlinie wird verwendet 380
Einzelheiten zur Richtlinie 380
Version der Richtlinie 380
JSON-Richtliniendokument 380
Weitere Informationen 408
AmazonDataZoneSageMakerManageAccessRolePolicy 408
Diese Richtlinie wird verwendet 408
Einzelheiten zur Richtlinie 408
Version der Richtlinie 408
JSON-Richtliniendokument 409
Weitere Informationen 413
AmazonDataZoneSageMakerProvisioningRolePolicy 414
Diese Richtlinie wird verwendet 414
Einzelheiten zur Richtlinie 414
Version der Richtlinie 414
JSON-Richtliniendokument 414
Weitere Informationen 419
AmazonDetectiveFullAccess 419
Diese Richtlinie wird verwendet 419
Einzelheiten zur Richtlinie 419
Version der Richtlinie 420
JSON-Richtliniendokument 420
Weitere Informationen 421
AmazonDetectiveInvestigatorAccess 421
Diese Richtlinie wird verwendet 421
Einzelheiten zur Richtlinie 421
Version der Richtlinie 422
JSON-Richtliniendokument 422
Weitere Informationen 423
AmazonDetectiveMemberAccess 424
Diese Richtlinie wird verwendet 424
Einzelheiten zur Richtlinie 424
Version der Richtlinie 424
JSON-Richtliniendokument 424
Weitere Informationen 425

AmazonDetectiveOrganizationsAccess 425
Diese Richtlinie wird verwendet 425
Einzelheiten zur Richtlinie 425
Version der Richtlinie 426
JSON-Richtliniendokument 426
Weitere Informationen 427
AmazonDetectiveServiceLinkedRolePolicy 428
Diese Richtlinie wird verwendet 428
Einzelheiten der Richtlinie 428
Version der Richtlinie 428
JSON-Richtliniendokument 428
Weitere Informationen 429
AmazonDevOpsGuruConsoleFullAccess 429
Diese Richtlinie wird verwendet 429
Einzelheiten zur Richtlinie 429
Version der Richtlinie 429
JSON-Richtliniendokument 430
Weitere Informationen 432
AmazonDevOpsGuruFullAccess 432
Diese Richtlinie wird verwendet 432
Einzelheiten zur Richtlinie 433
Version der Richtlinie 433
JSON-Richtliniendokument 433
Weitere Informationen 435
AmazonDevOpsGuruOrganizationsAccess 435
Diese Richtlinie wird verwendet 436
Einzelheiten zur Richtlinie 436
Version der Richtlinie 436
JSON-Richtliniendokument 436
Weitere Informationen 437
AmazonDevOpsGuruReadOnlyAccess 438
Diese Richtlinie wird verwendet 438
Einzelheiten zur Richtlinie 438
Version der Richtlinie 438
JSON-Richtliniendokument 438
Weitere Informationen 440

AmazonDevOpsGuruServiceRolePolicy 440
Diese Richtlinie wird verwendet 441
Einzelheiten der Richtlinie 441
Version der Richtlinie 441
JSON-Richtliniendokument 441
Weitere Informationen 445
AmazonDMSCloudWatchLogsRole 445
Diese Richtlinie wird verwendet 446
Einzelheiten zur Richtlinie 446
Version der Richtlinie 446
JSON-Richtliniendokument 446
Weitere Informationen 448
AmazonDMSRedshiftS3Role 448
Diese Richtlinie wird verwendet 448
Einzelheiten zur Richtlinie 448
Version der Richtlinie 448
JSON-Richtliniendokument 449
Weitere Informationen 449
AmazonDMSVPCManagementRole 450
Diese Richtlinie wird verwendet 450
Einzelheiten zur Richtlinie 450
Version der Richtlinie 450
JSON-Richtliniendokument 450
Weitere Informationen 451
AmazonDocDB-ElasticServiceRolePolicy 451
Diese Richtlinie wird verwendet 451
Einzelheiten der Richtlinie 451
Version der Richtlinie 452
JSON-Richtliniendokument 452
Weitere Informationen 452
AmazonDocDBConsoleFullAccess 453
Diese Richtlinie wird verwendet 453
Einzelheiten zur Richtlinie 453
Version der Richtlinie 453
JSON-Richtliniendokument 453
Weitere Informationen 458

AmazonDocDBElasticFullAccess 458
Diese Richtlinie wird verwendet 458
Einzelheiten zur Richtlinie 458
Version der Richtlinie 458
JSON-Richtliniendokument 459
Weitere Informationen 462
AmazonDocDBElasticReadOnlyAccess 462
Diese Richtlinie wird verwendet 462
Einzelheiten zur Richtlinie 462
Version der Richtlinie 463
JSON-Richtliniendokument 463
Weitere Informationen 464
AmazonDocDBFullAccess 464
Diese Richtlinie wird verwendet 464
Einzelheiten zur Richtlinie 464
Version der Richtlinie 464
JSON-Richtliniendokument 465
Weitere Informationen 467
AmazonDocDBReadOnlyAccess 468
Diese Richtlinie wird verwendet 468
Einzelheiten zur Richtlinie 468
Version der Richtlinie 468
JSON-Richtliniendokument 468
Weitere Informationen 470
AmazonDRSVPCManagement 470
Diese Richtlinie wird verwendet 470
Einzelheiten zur Richtlinie 471
Version der Richtlinie 471
JSON-Richtliniendokument 471
Weitere Informationen 472
AmazonDynamoDBFullAccess 472
Diese Richtlinie wird verwendet 472
Einzelheiten zur Richtlinie 472
Version der Richtlinie 472
JSON-Richtliniendokument 473
Weitere Informationen 475

AmazonDynamoDBFullAccess_v2 475
Diese Richtlinie wird verwendet 476
Einzelheiten zur Richtlinie 476
Version der Richtlinie 476
JSON-Richtliniendokument 476
Weitere Informationen 479
AmazonDynamoDBFullAccesswithDataPipeline 480
Diese Richtlinie wird verwendet 480
Einzelheiten zur Richtlinie 480
Version der Richtlinie 480
JSON-Richtliniendokument 480
Weitere Informationen 482
AmazonDynamoDBReadOnlyAccess 483
Diese Richtlinie wird verwendet 483
Einzelheiten zur Richtlinie 483
Version der Richtlinie 483
JSON-Richtliniendokument 483
Weitere Informationen 485
AmazonEBSCSIDriverPolicy 485
Diese Richtlinie wird verwendet 485
Einzelheiten zur Richtlinie 485
Version der Richtlinie 486
JSON-Richtliniendokument 486
Weitere Informationen 490
AmazonEC2ContainerRegistryFullAccess 491
Diese Richtlinie wird verwendet 491
Einzelheiten zur Richtlinie 491
Version der Richtlinie 491
JSON-Richtliniendokument 491
Weitere Informationen 492
AmazonEC2ContainerRegistryPowerUser 492
Diese Richtlinie wird verwendet 492
Einzelheiten zur Richtlinie 492
Version der Richtlinie 493
JSON-Richtliniendokument 493
Weitere Informationen 494

AmazonEC2ContainerRegistryPullOnly 494
Diese Richtlinie wird verwendet 494
Einzelheiten zur Richtlinie 494
Version der Richtlinie 494
JSON-Richtliniendokument 495
Weitere Informationen 495
AmazonEC2ContainerRegistryReadOnly 495
Diese Richtlinie wird verwendet 495
Einzelheiten zur Richtlinie 496
Version der Richtlinie 496
JSON-Richtliniendokument 496
Weitere Informationen 497
AmazonEC2ContainerServiceAutoscaleRole 497
Diese Richtlinie wird verwendet 497
Einzelheiten zur Richtlinie 497
Version der Richtlinie 497
JSON-Richtliniendokument 498
Weitere Informationen 498
AmazonEC2ContainerServiceEventsRole 498
Diese Richtlinie wird verwendet 499
Einzelheiten zur Richtlinie 499
Version der Richtlinie 499
JSON-Richtliniendokument 499
Weitere Informationen 500
AmazonEC2ContainerServiceforEC2Role 500
Diese Richtlinie wird verwendet 501
Einzelheiten zur Richtlinie 501
Version der Richtlinie 501
JSON-Richtliniendokument 501
Weitere Informationen 502
AmazonEC2ContainerServiceRole 503
Diese Richtlinie wird verwendet 503
Einzelheiten zur Richtlinie 503
Version der Richtlinie 503
JSON-Richtliniendokument 503
Weitere Informationen 504

AmazonEC2FullAccess 504
Diese Richtlinie wird verwendet 504
Einzelheiten zur Richtlinie 504
Version der Richtlinie 504
JSON-Richtliniendokument 505
Weitere Informationen 506
AmazonEC2ImageReferencesAccessPolicy 506
Diese Richtlinie wird verwendet 506
Einzelheiten zur Richtlinie 506
Version der Richtlinie 506
JSON-Richtliniendokument 507
Weitere Informationen 507
AmazonEC2ReadOnlyAccess 508
Diese Richtlinie wird verwendet 508
Einzelheiten zur Richtlinie 508
Version der Richtlinie 508
JSON-Richtliniendokument 508
Weitere Informationen 509
AmazonEC2RoleforAWSCodeDeploy 509
Diese Richtlinie wird verwendet 510
Einzelheiten zur Richtlinie 510
Version der Richtlinie 510
JSON-Richtliniendokument 510
Weitere Informationen 511
AmazonEC2RoleforAWSCodeDeployLimited 511
Diese Richtlinie wird verwendet 511
Einzelheiten zur Richtlinie 511
Version der Richtlinie 511
JSON-Richtliniendokument 512
Weitere Informationen 512
AmazonEC2RoleforDataPipelineRole 513
Diese Richtlinie wird verwendet 513
Einzelheiten zur Richtlinie 513
Version der Richtlinie 513
JSON-Richtliniendokument 513
Weitere Informationen 514

AmazonEC2RoleforSSM 514
Diese Richtlinie wird verwendet 514
Einzelheiten zur Richtlinie 515
Version der Richtlinie 515
JSON-Richtliniendokument 515
Weitere Informationen 517
AmazonEC2RolePolicyForLaunchWizard 517
Diese Richtlinie wird verwendet 518
Einzelheiten zur Richtlinie 518
Version der Richtlinie 518
JSON-Richtliniendokument 518
Weitere Informationen 522
AmazonEC2SpotFleetAutoscaleRole 522
Diese Richtlinie wird verwendet 522
Einzelheiten zur Richtlinie 523
Version der Richtlinie 523
JSON-Richtliniendokument 523
Weitere Informationen 524
AmazonEC2SpotFleetTaggingRole 524
Diese Richtlinie wird verwendet 524
Einzelheiten zur Richtlinie 524
Version der Richtlinie 525
JSON-Richtliniendokument 525
Weitere Informationen 526
AmazonECS_FullAccess 526
Diese Richtlinie wird verwendet 527
Einzelheiten zur Richtlinie 527
Version der Richtlinie 527
JSON-Richtliniendokument 527
Weitere Informationen 533
AmazonECSComputeServiceRolePolicy 533
Diese Richtlinie wird verwendet 533
Einzelheiten der Richtlinie 533
Version der Richtlinie 534
JSON-Richtliniendokument 534
Weitere Informationen 535

AmazonECSInfrastructureRoleforExpressGatewayServices 536
Diese Richtlinie wird verwendet 536
Einzelheiten zur Richtlinie 536
Version der Richtlinie 536
JSON-Richtliniendokument 536
Weitere Informationen 543
AmazonECSInfrastructureRolePolicyForLoadBalancers 543
Diese Richtlinie wird verwendet 543
Einzelheiten zur Richtlinie 543
Version der Richtlinie 543
JSON-Richtliniendokument 544
Weitere Informationen 545
AmazonECSInfrastructureRolePolicyForManagedInstances 545
Diese Richtlinie wird verwendet 545
Einzelheiten zur Richtlinie 545
Version der Richtlinie 546
JSON-Richtliniendokument 546
Weitere Informationen 550
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity 550
Diese Richtlinie wird verwendet 550
Einzelheiten zur Richtlinie 551
Version der Richtlinie 551
JSON-Richtliniendokument 551
Weitere Informationen 553
AmazonECSInfrastructureRolePolicyForVolumes 554
Diese Richtlinie wird verwendet 554
Einzelheiten zur Richtlinie 554
Version der Richtlinie 554
JSON-Richtliniendokument 554
Weitere Informationen 557
AmazonECSInfrastructureRolePolicyForVpcLattice 557
Diese Richtlinie wird verwendet 557
Einzelheiten zur Richtlinie 557
Version der Richtlinie 557
JSON-Richtliniendokument 558
Weitere Informationen 559

AmazonECSInstanceRolePolicyForManagedInstances 559
Diese Richtlinie wird verwendet 559
Einzelheiten zur Richtlinie 559
Version der Richtlinie 560
JSON-Richtliniendokument 560
Weitere Informationen 561
AmazonECSServiceRolePolicy 561
Diese Richtlinie wird verwendet 561
Einzelheiten der Richtlinie 561
Version der Richtlinie 562
JSON-Richtliniendokument 562
Weitere Informationen 567
AmazonECSTaskExecutionRolePolicy 567
Diese Richtlinie wird verwendet 568
Einzelheiten zur Richtlinie 568
Version der Richtlinie 568
JSON-Richtliniendokument 568
Weitere Informationen 569
AmazonEFSCSIDriverPolicy 569
Diese Richtlinie wird verwendet 569
Einzelheiten zur Richtlinie 569
Version der Richtlinie 569
JSON-Richtliniendokument 570
Weitere Informationen 571
AmazonEKS_CNI_Policy 571
Diese Richtlinie wird verwendet 572
Einzelheiten zur Richtlinie 572
Version der Richtlinie 572
JSON-Richtliniendokument 572
Weitere Informationen 573
AmazonEKSBlockStoragePolicy 573
Diese Richtlinie wird verwendet 573
Einzelheiten zur Richtlinie 573
Version der Richtlinie 574
JSON-Richtliniendokument 574
Weitere Informationen 576

AmazonEKSClusterPolicy 576
Diese Richtlinie wird verwendet 577
Einzelheiten zur Richtlinie 577
Version der Richtlinie 577
JSON-Richtliniendokument 577
Weitere Informationen 579
AmazonEKSComputePolicy 580
Diese Richtlinie wird verwendet 580
Einzelheiten zur Richtlinie 580
Version der Richtlinie 580
JSON-Richtliniendokument 580
Weitere Informationen 583
AmazonEKSConnectorServiceRolePolicy 583
Diese Richtlinie wird verwendet 583
Einzelheiten der Richtlinie 583
Version der Richtlinie 584
JSON-Richtliniendokument 584
Weitere Informationen 586
AmazonEKSDashboardConsoleReadOnly 586
Diese Richtlinie wird verwendet 586
Einzelheiten zur Richtlinie 586
Version der Richtlinie 587
JSON-Richtliniendokument 587
Weitere Informationen 588
AmazonEKSDashboardServiceRolePolicy 588
Diese Richtlinie wird verwendet 588
Einzelheiten der Richtlinie 588
Version der Richtlinie 589
JSON-Richtliniendokument 589
Weitere Informationen 589
AmazonEKSFargatePodExecutionRolePolicy 590
Diese Richtlinie wird verwendet 590
Einzelheiten zur Richtlinie 590
Version der Richtlinie 590
JSON-Richtliniendokument 590
Weitere Informationen 591

AmazonEKSForFargateServiceRolePolicy 591
Diese Richtlinie wird verwendet 591
Einzelheiten der Richtlinie 591
Version der Richtlinie 592
JSON-Richtliniendokument 592
Weitere Informationen 592
AmazonEKSLoadBalancingPolicy 593
Diese Richtlinie wird verwendet 593
Einzelheiten zur Richtlinie 593
Version der Richtlinie 593
JSON-Richtliniendokument 593
Weitere Informationen 599
AmazonEKSLocalOutpostClusterPolicy 600
Diese Richtlinie wird verwendet 600
Einzelheiten zur Richtlinie 600
Version der Richtlinie 600
JSON-Richtliniendokument 600
Weitere Informationen 602
AmazonEKSLocalOutpostServiceRolePolicy 602
Diese Richtlinie wird verwendet 603
Einzelheiten der Richtlinie 603
Version der Richtlinie 603
JSON-Richtliniendokument 603
Weitere Informationen 609
AmazonEKSMCPReadOnlyAccess 609
Diese Richtlinie wird verwendet 609
Einzelheiten zur Richtlinie 609
Version der Richtlinie 610
JSON-Richtliniendokument 610
Weitere Informationen 612
AmazonEKSNetworkingPolicy 612
Diese Richtlinie wird verwendet 612
Einzelheiten zur Richtlinie 612
Version der Richtlinie 612
JSON-Richtliniendokument 613
Weitere Informationen 614

AmazonEKSServicePolicy 614
Diese Richtlinie wird verwendet 614
Einzelheiten zur Richtlinie 615
Version der Richtlinie 615
JSON-Richtliniendokument 615
Weitere Informationen 617
AmazonEKSServiceRolePolicy 617
Diese Richtlinie wird verwendet 617
Einzelheiten der Richtlinie 618
Version der Richtlinie 618
JSON-Richtliniendokument 618
Weitere Informationen 626
AmazonEKSVPCResourceController 626
Diese Richtlinie wird verwendet 626
Einzelheiten zur Richtlinie 626
Version der Richtlinie 626
JSON-Richtliniendokument 626
Weitere Informationen 627
AmazonEKSWorkerNodeMinimalPolicy 627
Diese Richtlinie wird verwendet 628
Einzelheiten zur Richtlinie 628
Version der Richtlinie 628
JSON-Richtliniendokument 628
Weitere Informationen 629
AmazonEKSWorkerNodePolicy 629
Diese Richtlinie wird verwendet 629
Einzelheiten zur Richtlinie 629
Version der Richtlinie 629
JSON-Richtliniendokument 630
Weitere Informationen 630
AmazonElastiCacheFullAccess 630
Diese Richtlinie wird verwendet 631
Einzelheiten zur Richtlinie 631
Version der Richtlinie 631
JSON-Richtliniendokument 631
Weitere Informationen 634

AmazonElastiCacheReadOnlyAccess 635
Diese Richtlinie wird verwendet 635
Einzelheiten zur Richtlinie 635
Version der Richtlinie 635
JSON-Richtliniendokument 635
Weitere Informationen 636
AmazonElasticContainerRegistryPublicFullAccess 636
Diese Richtlinie wird verwendet 636
Einzelheiten zur Richtlinie 636
Version der Richtlinie 636
JSON-Richtliniendokument 637
Weitere Informationen 637
AmazonElasticContainerRegistryPublicPowerUser 637
Diese Richtlinie wird verwendet 637
Einzelheiten zur Richtlinie 638
Version der Richtlinie 638
JSON-Richtliniendokument 638
Weitere Informationen 639
AmazonElasticContainerRegistryPublicReadOnly 639
Diese Richtlinie wird verwendet 639
Einzelheiten zur Richtlinie 639
Version der Richtlinie 639
JSON-Richtliniendokument 640
Weitere Informationen 640
AmazonElasticFileSystemClientFullAccess 640
Diese Richtlinie wird verwendet 641
Einzelheiten zur Richtlinie 641
Version der Richtlinie 641
JSON-Richtliniendokument 641
Weitere Informationen 642
AmazonElasticFileSystemClientReadOnlyAccess 642
Diese Richtlinie wird verwendet 642
Einzelheiten zur Richtlinie 642
Version der Richtlinie 642
JSON-Richtliniendokument 643
Weitere Informationen 643

AmazonElasticFileSystemClientReadWriteAccess 643
Diese Richtlinie wird verwendet 643
Einzelheiten zur Richtlinie 643
Version der Richtlinie 644
JSON-Richtliniendokument 644
Weitere Informationen 644
AmazonElasticFileSystemFullAccess 645
Diese Richtlinie wird verwendet 645
Einzelheiten zur Richtlinie 645
Version der Richtlinie 645
JSON-Richtliniendokument 645
Weitere Informationen 647
AmazonElasticFileSystemReadOnlyAccess 648
Diese Richtlinie wird verwendet 648
Einzelheiten zur Richtlinie 648
Version der Richtlinie 648
JSON-Richtliniendokument 648
Weitere Informationen 649
AmazonElasticFileSystemServiceRolePolicy 649
Diese Richtlinie wird verwendet 650
Einzelheiten der Richtlinie 650
Version der Richtlinie 650
JSON-Richtliniendokument 650
Weitere Informationen 652
AmazonElasticFileSystemsUtils 652
Diese Richtlinie wird verwendet 653
Einzelheiten zur Richtlinie 653
Version der Richtlinie 653
JSON-Richtliniendokument 653
Weitere Informationen 655
AmazonElasticMapReduceEditorsRole 655
Diese Richtlinie wird verwendet 655
Einzelheiten zur Richtlinie 655
Version der Richtlinie 656
JSON-Richtliniendokument 656
Weitere Informationen 657

AmazonElasticMapReduceforAutoScalingRole 657
Diese Richtlinie wird verwendet 657
Einzelheiten zur Richtlinie 657
Version der Richtlinie 658
JSON-Richtliniendokument 658
Weitere Informationen 658
AmazonElasticMapReduceforEC2Role 659
Diese Richtlinie wird verwendet 659
Einzelheiten zur Richtlinie 659
Version der Richtlinie 659
JSON-Richtliniendokument 659
Weitere Informationen 661
AmazonElasticMapReduceFullAccess 661
Diese Richtlinie wird verwendet 661
Einzelheiten zur Richtlinie 661
Version der Richtlinie 661
JSON-Richtliniendokument 662
Weitere Informationen 663
AmazonElasticMapReducePlacementGroupPolicy 664
Diese Richtlinie wird verwendet 664
Einzelheiten zur Richtlinie 664
Version der Richtlinie 664
JSON-Richtliniendokument 664
Weitere Informationen 665
AmazonElasticMapReduceReadOnlyAccess 665
Diese Richtlinie wird verwendet 665
Einzelheiten zur Richtlinie 665
Version der Richtlinie 666
JSON-Richtliniendokument 666
Weitere Informationen 666
AmazonElasticMapReduceRole 667
Diese Richtlinie wird verwendet 667
Einzelheiten zur Richtlinie 667
Version der Richtlinie 667
JSON-Richtliniendokument 667
Weitere Informationen 669

AmazonElasticsearchServiceRolePolicy 670
Diese Richtlinie wird verwendet 670
Einzelheiten der Richtlinie 670
Version der Richtlinie 670
JSON-Richtliniendokument 670
Weitere Informationen 673
AmazonElasticTranscoder_FullAccess 673
Diese Richtlinie wird verwendet 674
Einzelheiten zur Richtlinie 674
Version der Richtlinie 674
JSON-Richtliniendokument 674
Weitere Informationen 675
AmazonElasticTranscoder_JobsSubmitter 675
Diese Richtlinie wird verwendet 675
Einzelheiten zur Richtlinie 675
Version der Richtlinie 676
JSON-Richtliniendokument 676
Weitere Informationen 676
AmazonElasticTranscoder_ReadOnlyAccess 677
Diese Richtlinie wird verwendet 677
Einzelheiten zur Richtlinie 677
Version der Richtlinie 677
JSON-Richtliniendokument 677
Weitere Informationen 678
AmazonElasticTranscoderRole 678
Diese Richtlinie wird verwendet 678
Einzelheiten zur Richtlinie 678
Version der Richtlinie 679
JSON-Richtliniendokument 679
Weitere Informationen 680
AmazonEMRCleanupPolicy 680
Diese Richtlinie wird verwendet 680
Einzelheiten der Richtlinie 680
Version der Richtlinie 680
JSON-Richtliniendokument 681
Weitere Informationen 681

AmazonEMRContainersServiceRolePolicy 682
Diese Richtlinie wird verwendet 682
Einzelheiten der Richtlinie 682
Version der Richtlinie 682
JSON-Richtliniendokument 682
Weitere Informationen 684
AmazonEMRFullAccessPolicy_v2 684
Diese Richtlinie wird verwendet 684
Einzelheiten zur Richtlinie 684
Version der Richtlinie 684
JSON-Richtliniendokument 684
Weitere Informationen 688
AmazonEMRReadOnlyAccessPolicy_v2 688
Diese Richtlinie wird verwendet 688
Einzelheiten zur Richtlinie 688
Version der Richtlinie 689
JSON-Richtliniendokument 689
Weitere Informationen 690
AmazonEMRServerlessServiceRolePolicy 690
Diese Richtlinie wird verwendet 690
Einzelheiten der Richtlinie 690
Version der Richtlinie 691
JSON-Richtliniendokument 691
Weitere Informationen 692
AmazonEMRServicePolicy_v2 692
Diese Richtlinie wird verwendet 692
Einzelheiten zur Richtlinie 692
Version der Richtlinie 692
JSON-Richtliniendokument 693
Weitere Informationen 701
AmazonESCognitoAccess 702
Diese Richtlinie wird verwendet 702
Einzelheiten zur Richtlinie 702
Version der Richtlinie 702
JSON-Richtliniendokument 702
Weitere Informationen 703

AmazonESFullAccess ... 703
Diese Richtlinie wird verwendet ... 704
Einzelheiten zur Richtlinie ... 704
Version der Richtlinie ... 704
JSON-Richtliniendokument ... 704
Weitere Informationen ... 704
AmazonESReadOnlyAccess ... 705
Diese Richtlinie wird verwendet ... 705
Einzelheiten zur Richtlinie ... 705
Version der Richtlinie ... 705
JSON-Richtliniendokument ... 705
Weitere Informationen ... 706
AmazonEventBridgeApiDestinationsServiceRolePolicy ... 706
Diese Richtlinie wird verwendet ... 706
Einzelheiten der Richtlinie ... 706
Version der Richtlinie ... 707
JSON-Richtliniendokument ... 707
Weitere Informationen ... 708
AmazonEventBridgeFullAccess ... 708
Diese Richtlinie wird verwendet ... 708
Einzelheiten zur Richtlinie ... 708
Version der Richtlinie ... 708
JSON-Richtliniendokument ... 709
Weitere Informationen ... 711
AmazonEventBridgePipesFullAccess ... 711
Diese Richtlinie wird verwendet ... 711
Einzelheiten zur Richtlinie ... 711
Version der Richtlinie ... 711
JSON-Richtliniendokument ... 712
Weitere Informationen ... 712
AmazonEventBridgePipesOperatorAccess ... 713
Diese Richtlinie wird verwendet ... 713
Einzelheiten zur Richtlinie ... 713
Version der Richtlinie ... 713
JSON-Richtliniendokument ... 713
Weitere Informationen ... 714

AmazonEventBridgePipesReadOnlyAccess 714
Diese Richtlinie wird verwendet 714
Einzelheiten zur Richtlinie 714
Version der Richtlinie 714
JSON-Richtliniendokument 715
Weitere Informationen 715
AmazonEventBridgeReadOnlyAccess 715
Diese Richtlinie wird verwendet 716
Einzelheiten zur Richtlinie 716
Version der Richtlinie 716
JSON-Richtliniendokument 716
Weitere Informationen 717
AmazonEventBridgeSchedulerFullAccess 718
Diese Richtlinie wird verwendet 718
Einzelheiten zur Richtlinie 718
Version der Richtlinie 718
JSON-Richtliniendokument 718
Weitere Informationen 719
AmazonEventBridgeSchedulerReadOnlyAccess 719
Diese Richtlinie wird verwendet 719
Einzelheiten zur Richtlinie 719
Version der Richtlinie 720
JSON-Richtliniendokument 720
Weitere Informationen 720
AmazonEventBridgeSchemasFullAccess 721
Diese Richtlinie wird verwendet 721
Einzelheiten zur Richtlinie 721
Version der Richtlinie 721
JSON-Richtliniendokument 721
Weitere Informationen 722
AmazonEventBridgeSchemasReadOnlyAccess 722
Diese Richtlinie wird verwendet 723
Einzelheiten zur Richtlinie 723
Version der Richtlinie 723
JSON-Richtliniendokument 723
Weitere Informationen 724

AmazonEventBridgeSchemasServiceRolePolicy 724
Diese Richtlinie wird verwendet 724
Einzelheiten der Richtlinie 724
Version der Richtlinie 725
JSON-Richtliniendokument 725
Weitere Informationen 725
AmazonEVSServiceRolePolicy 726
Diese Richtlinie wird verwendet 726
Einzelheiten der Richtlinie 726
Version der Richtlinie 726
JSON-Richtliniendokument 726
Weitere Informationen 730
AmazonFISServiceRolePolicy 730
Diese Richtlinie wird verwendet 731
Einzelheiten der Richtlinie 731
Version der Richtlinie 731
JSON-Richtliniendokument 731
Weitere Informationen 733
AmazonForecastFullAccess 733
Diese Richtlinie wird verwendet 733
Einzelheiten zur Richtlinie 733
Version der Richtlinie 733
JSON-Richtliniendokument 734
Weitere Informationen 734
AmazonFraudDetectorFullAccessPolicy 734
Diese Richtlinie wird verwendet 735
Einzelheiten zur Richtlinie 735
Version der Richtlinie 735
JSON-Richtliniendokument 735
Weitere Informationen 736
AmazonFreeRTOSFullAccess 737
Diese Richtlinie wird verwendet 737
Einzelheiten zur Richtlinie 737
Version der Richtlinie 737
JSON-Richtliniendokument 737
Weitere Informationen 738

AmazonFreeRTOSOTAUpdate 738
Diese Richtlinie wird verwendet 738
Einzelheiten zur Richtlinie 738
Version der Richtlinie 738
JSON-Richtliniendokument 739
Weitere Informationen 740
AmazonFSxConsoleFullAccess 740
Diese Richtlinie wird verwendet 740
Einzelheiten zur Richtlinie 740
Version der Richtlinie 741
JSON-Richtliniendokument 741
Weitere Informationen 744
AmazonFSxConsoleReadOnlyAccess 745
Diese Richtlinie wird verwendet 745
Einzelheiten zur Richtlinie 745
Version der Richtlinie 745
JSON-Richtliniendokument 745
Weitere Informationen 746
AmazonFSxFullAccess 746
Diese Richtlinie wird verwendet 746
Einzelheiten zur Richtlinie 746
Version der Richtlinie 747
JSON-Richtliniendokument 747
Weitere Informationen 751
AmazonFSxReadOnlyAccess 751
Diese Richtlinie wird verwendet 751
Einzelheiten zur Richtlinie 751
Version der Richtlinie 752
JSON-Richtliniendokument 752
Weitere Informationen 752
AmazonFSxServiceRolePolicy 752
Diese Richtlinie wird verwendet 753
Einzelheiten der Richtlinie 753
Version der Richtlinie 753
JSON-Richtliniendokument 753
Weitere Informationen 756

AmazonGlacierFullAccess 756
Diese Richtlinie wird verwendet 756
Einzelheiten zur Richtlinie 756
Version der Richtlinie 757
JSON-Richtliniendokument 757
Weitere Informationen 757
AmazonGlacierReadOnlyAccess 757
Diese Richtlinie wird verwendet 758
Einzelheiten zur Richtlinie 758
Version der Richtlinie 758
JSON-Richtliniendokument 758
Weitere Informationen 759
AmazonGrafanaAthenaAccess 759
Diese Richtlinie wird verwendet 759
Einzelheiten zur Richtlinie 759
Version der Richtlinie 759
JSON-Richtliniendokument 760
Weitere Informationen 761
AmazonGrafanaCloudWatchAccess 762
Diese Richtlinie wird verwendet 762
Einzelheiten zur Richtlinie 762
Version der Richtlinie 762
JSON-Richtliniendokument 762
Weitere Informationen 764
AmazonGrafanaRedshiftAccess 764
Diese Richtlinie wird verwendet 764
Einzelheiten zur Richtlinie 764
Version der Richtlinie 764
JSON-Richtliniendokument 765
Weitere Informationen 766
AmazonGrafanaServiceLinkedRolePolicy 766
Diese Richtlinie wird verwendet 766
Einzelheiten der Richtlinie 766
Version der Richtlinie 767
JSON-Richtliniendokument 767
Weitere Informationen 768

AmazonGuardDutyFullAccess 768
Diese Richtlinie wird verwendet 768
Einzelheiten zur Richtlinie 768
Version der Richtlinie 769
JSON-Richtliniendokument 769
Weitere Informationen 770
AmazonGuardDutyFullAccess_v2 771
Diese Richtlinie wird verwendet 771
Einzelheiten zur Richtlinie 771
Version der Richtlinie 771
JSON-Richtliniendokument 771
Weitere Informationen 773
AmazonGuardDutyMalwareProtectionServiceRolePolicy 774
Diese Richtlinie wird verwendet 774
Einzelheiten der Richtlinie 774
Version der Richtlinie 774
JSON-Richtliniendokument 775
Weitere Informationen 779
AmazonGuardDutyReadOnlyAccess 779
Diese Richtlinie wird verwendet 779
Einzelheiten zur Richtlinie 779
Version der Richtlinie 780
JSON-Richtliniendokument 780
Weitere Informationen 780
AmazonGuardDutyServiceRolePolicy 781
Diese Richtlinie wird verwendet 781
Einzelheiten der Richtlinie 781
Version der Richtlinie 781
JSON-Richtliniendokument 782
Weitere Informationen 788
AmazonHealthLakeFullAccess 788
Diese Richtlinie wird verwendet 788
Einzelheiten zur Richtlinie 788
Version der Richtlinie 788
JSON-Richtliniendokument 788
Weitere Informationen 789

AmazonHealthLakeReadOnlyAccess 789
Diese Richtlinie wird verwendet 789
Einzelheiten zur Richtlinie 790
Version der Richtlinie 790
JSON-Richtliniendokument 790
Weitere Informationen 791
AmazonHoneycodeFullAccess 791
Diese Richtlinie wird verwendet 791
Einzelheiten zur Richtlinie 791
Version der Richtlinie 791
JSON-Richtliniendokument 791
Weitere Informationen 792
AmazonHoneycodeReadOnlyAccess 792
Diese Richtlinie wird verwendet 792
Einzelheiten zur Richtlinie 792
Version der Richtlinie 793
JSON-Richtliniendokument 793
Weitere Informationen 793
AmazonHoneycodeServiceRolePolicy 793
Diese Richtlinie wird verwendet 794
Einzelheiten der Richtlinie 794
Version der Richtlinie 794
JSON-Richtliniendokument 794
Weitere Informationen 795
AmazonHoneycodeTeamAssociationFullAccess 795
Diese Richtlinie wird verwendet 795
Einzelheiten zur Richtlinie 795
Version der Richtlinie 795
JSON-Richtliniendokument 795
Weitere Informationen 796
AmazonHoneycodeTeamAssociationReadOnlyAccess 796
Diese Richtlinie wird verwendet 796
Einzelheiten zur Richtlinie 796
Version der Richtlinie 797
JSON-Richtliniendokument 797
Weitere Informationen 797

AmazonHoneycodeWorkbookFullAccess 797
Diese Richtlinie wird verwendet 798
Einzelheiten zur Richtlinie 798
Version der Richtlinie 798
JSON-Richtliniendokument 798
Weitere Informationen 799
AmazonHoneycodeWorkbookReadOnlyAccess 799
Diese Richtlinie wird verwendet 799
Einzelheiten zur Richtlinie 799
Version der Richtlinie 800
JSON-Richtliniendokument 800
Weitere Informationen 800
AmazonInspector2AgentlessServiceRolePolicy 801
Diese Richtlinie wird verwendet 801
Einzelheiten der Richtlinie 801
Version der Richtlinie 801
JSON-Richtliniendokument 801
Weitere Informationen 805
AmazonInspector2FullAccess 805
Diese Richtlinie wird verwendet 805
Einzelheiten zur Richtlinie 805
Version der Richtlinie 806
JSON-Richtliniendokument 806
Weitere Informationen 807
AmazonInspector2FullAccess_v2 807
Diese Richtlinie wird verwendet 807
Einzelheiten zur Richtlinie 807
Version der Richtlinie 808
JSON-Richtliniendokument 808
Weitere Informationen 810
AmazonInspector2ManagedCisPolicy 811
Diese Richtlinie wird verwendet 811
Einzelheiten zur Richtlinie 811
Version der Richtlinie 811
JSON-Richtliniendokument 811
Weitere Informationen 812

AmazonInspector2ReadOnlyAccess 812
Diese Richtlinie wird verwendet 812
Einzelheiten zur Richtlinie 812
Version der Richtlinie 813
JSON-Richtliniendokument 813
Weitere Informationen 814
AmazonInspector2ServiceRolePolicy 814
Diese Richtlinie wird verwendet 815
Einzelheiten der Richtlinie 815
Version der Richtlinie 815
JSON-Richtliniendokument 815
Weitere Informationen 823
AmazonInspectorFullAccess 823
Diese Richtlinie wird verwendet 823
Einzelheiten zur Richtlinie 824
Version der Richtlinie 824
JSON-Richtliniendokument 824
Weitere Informationen 825
AmazonInspectorReadOnlyAccess 825
Diese Richtlinie wird verwendet 825
Einzelheiten zur Richtlinie 826
Version der Richtlinie 826
JSON-Richtliniendokument 826
Weitere Informationen 827
AmazonInspectorServiceRolePolicy 827
Diese Richtlinie wird verwendet 827
Einzelheiten der Richtlinie 827
Version der Richtlinie 827
JSON-Richtliniendokument 828
Weitere Informationen 829
AmazonKendraFullAccess 829
Diese Richtlinie wird verwendet 829
Einzelheiten zur Richtlinie 829
Version der Richtlinie 830
JSON-Richtliniendokument 830
Weitere Informationen 832

AmazonKendraReadOnlyAccess 832
Diese Richtlinie wird verwendet 832
Einzelheiten zur Richtlinie 832
Version der Richtlinie 832
JSON-Richtliniendokument 833
Weitere Informationen 833
AmazonKeyspacesFullAccess 833
Diese Richtlinie wird verwendet 833
Einzelheiten zur Richtlinie 833
Version der Richtlinie 834
JSON-Richtliniendokument 834
Weitere Informationen 836
AmazonKeyspacesReadOnlyAccess 836
Diese Richtlinie wird verwendet 836
Einzelheiten zur Richtlinie 837
Version der Richtlinie 837
JSON-Richtliniendokument 837
Weitere Informationen 838
AmazonKeyspacesReadOnlyAccess_v2 838
Diese Richtlinie wird verwendet 838
Einzelheiten zur Richtlinie 838
Version der Richtlinie 838
JSON-Richtliniendokument 839
Weitere Informationen 840
AmazonKinesisAnalyticsFullAccess 840
Diese Richtlinie wird verwendet 840
Einzelheiten zur Richtlinie 840
Version der Richtlinie 840
JSON-Richtliniendokument 841
Weitere Informationen 842
AmazonKinesisAnalyticsReadOnly 842
Diese Richtlinie wird verwendet 842
Einzelheiten zur Richtlinie 843
Version der Richtlinie 843
JSON-Richtliniendokument 843
Weitere Informationen 844

AmazonKinesisFirehoseFullAccess 845
Diese Richtlinie wird verwendet 845
Einzelheiten zur Richtlinie 845
Version der Richtlinie 845
JSON-Richtliniendokument 845
Weitere Informationen 846
AmazonKinesisFirehoseReadOnlyAccess 846
Diese Richtlinie wird verwendet 846
Einzelheiten zur Richtlinie 846
Version der Richtlinie 846
JSON-Richtliniendokument 847
Weitere Informationen 847
AmazonKinesisFullAccess 847
Diese Richtlinie wird verwendet 847
Einzelheiten zur Richtlinie 847
Version der Richtlinie 848
JSON-Richtliniendokument 848
Weitere Informationen 848
AmazonKinesisReadOnlyAccess 848
Diese Richtlinie wird verwendet 849
Einzelheiten zur Richtlinie 849
Version der Richtlinie 849
JSON-Richtliniendokument 849
Weitere Informationen 850
AmazonKinesisVideoStreamsFullAccess 850
Diese Richtlinie wird verwendet 850
Einzelheiten zur Richtlinie 850
Version der Richtlinie 850
JSON-Richtliniendokument 851
Weitere Informationen 851
AmazonKinesisVideoStreamsReadOnlyAccess 851
Diese Richtlinie wird verwendet 851
Einzelheiten zur Richtlinie 851
Version der Richtlinie 852
JSON-Richtliniendokument 852
Weitere Informationen 852

AmazonLaunchWizard_Fullaccess ... 853
Diese Richtlinie wird verwendet ... 853
Einzelheiten zur Richtlinie ... 853
Version der Richtlinie ... 853
JSON-Richtliniendokument ... 853
Weitere Informationen ... 867
AmazonLaunchWizardFullAccessV2 ... 868
Diese Richtlinie wird verwendet ... 868
Einzelheiten zur Richtlinie ... 868
Version der Richtlinie ... 868
JSON-Richtliniendokument ... 868
Weitere Informationen ... 885
AmazonLexChannelsAccess ... 885
Diese Richtlinie wird verwendet ... 885
Einzelheiten der Richtlinie ... 885
Version der Richtlinie ... 885
JSON-Richtliniendokument ... 886
Weitere Informationen ... 886
AmazonLexFullAccess ... 886
Diese Richtlinie wird verwendet ... 886
Einzelheiten zur Richtlinie ... 887
Version der Richtlinie ... 887
JSON-Richtliniendokument ... 887
Weitere Informationen ... 892
AmazonLexReadOnly ... 893
Diese Richtlinie wird verwendet ... 893
Einzelheiten zur Richtlinie ... 893
Version der Richtlinie ... 893
JSON-Richtliniendokument ... 893
Weitere Informationen ... 895
AmazonLexReplicationPolicy ... 895
Diese Richtlinie wird verwendet ... 895
Einzelheiten der Richtlinie ... 895
Version der Richtlinie ... 896
JSON-Richtliniendokument ... 896
Weitere Informationen ... 898

AmazonLexRunBotsOnly 898
Diese Richtlinie wird verwendet 898
Einzelheiten zur Richtlinie 898
Version der Richtlinie 899
JSON-Richtliniendokument 899
Weitere Informationen 899
AmazonLexV2BotPolicy 900
Diese Richtlinie wird verwendet 900
Einzelheiten der Richtlinie 900
Version der Richtlinie 900
JSON-Richtliniendokument 900
Weitere Informationen 901
AmazonLookoutEquipmentFullAccess 901
Diese Richtlinie wird verwendet 901
Einzelheiten zur Richtlinie 901
Version der Richtlinie 901
JSON-Richtliniendokument 902
Weitere Informationen 903
AmazonLookoutEquipmentReadOnlyAccess 903
Diese Richtlinie wird verwendet 903
Einzelheiten zur Richtlinie 903
Version der Richtlinie 904
JSON-Richtliniendokument 904
Weitere Informationen 904
AmazonLookoutMetricsFullAccess 904
Diese Richtlinie wird verwendet 905
Einzelheiten zur Richtlinie 905
Version der Richtlinie 905
JSON-Richtliniendokument 905
Weitere Informationen 906
AmazonLookoutMetricsReadOnlyAccess 906
Diese Richtlinie wird verwendet 906
Einzelheiten zur Richtlinie 906
Version der Richtlinie 906
JSON-Richtliniendokument 907
Weitere Informationen 907

AmazonLookoutVisionConsoleFullAccess 908
Diese Richtlinie wird verwendet 908
Einzelheiten zur Richtlinie 908
Version der Richtlinie 908
JSON-Richtliniendokument 908
Weitere Informationen 911
AmazonLookoutVisionConsoleReadOnlyAccess 911
Diese Richtlinie wird verwendet 911
Einzelheiten zur Richtlinie 911
Version der Richtlinie 911
JSON-Richtliniendokument 912
Weitere Informationen 913
AmazonLookoutVisionFullAccess 913
Diese Richtlinie wird verwendet 913
Einzelheiten zur Richtlinie 913
Version der Richtlinie 913
JSON-Richtliniendokument 914
Weitere Informationen 914
AmazonLookoutVisionReadOnlyAccess 914
Diese Richtlinie wird verwendet 915
Einzelheiten zur Richtlinie 915
Version der Richtlinie 915
JSON-Richtliniendokument 915
Weitere Informationen 916
AmazonMachineLearningBatchPredictionsAccess 916
Diese Richtlinie wird verwendet 916
Einzelheiten zur Richtlinie 916
Version der Richtlinie 916
JSON-Richtliniendokument 917
Weitere Informationen 917
AmazonMachineLearningCreateOnlyAccess 917
Diese Richtlinie wird verwendet 918
Einzelheiten zur Richtlinie 918
Version der Richtlinie 918
JSON-Richtliniendokument 918
Weitere Informationen 919

AmazonMachineLearningFullAccess 919
Diese Richtlinie wird verwendet 919
Einzelheiten zur Richtlinie 919
Version der Richtlinie 919
JSON-Richtliniendokument 920
Weitere Informationen 920
AmazonMachineLearningManageRealTimeEndpointOnlyAccess 920
Diese Richtlinie wird verwendet 920
Einzelheiten zur Richtlinie 920
Version der Richtlinie 921
JSON-Richtliniendokument 921
Weitere Informationen 921
AmazonMachineLearningReadOnlyAccess 922
Diese Richtlinie wird verwendet 922
Einzelheiten zur Richtlinie 922
Version der Richtlinie 922
JSON-Richtliniendokument 922
Weitere Informationen 923
AmazonMachineLearningRealTimePredictionOnlyAccess 923
Diese Richtlinie wird verwendet 923
Einzelheiten zur Richtlinie 923
Version der Richtlinie 923
JSON-Richtliniendokument 924
Weitere Informationen 924
AmazonMachineLearningRoleforRedshiftDataSourceV3 924
Diese Richtlinie wird verwendet 924
Einzelheiten zur Richtlinie 925
Version der Richtlinie 925
JSON-Richtliniendokument 925
Weitere Informationen 926
AmazonMacieFullAccess 926
Diese Richtlinie wird verwendet 926
Einzelheiten zur Richtlinie 926
Version der Richtlinie 927
JSON-Richtliniendokument 927
Weitere Informationen 928

AmazonMacieHandshakeRole 928
Diese Richtlinie wird verwendet 928
Einzelheiten zur Richtlinie 928
Version der Richtlinie 928
JSON-Richtliniendokument 928
Weitere Informationen 929
AmazonMacieReadOnlyAccess 929
Diese Richtlinie wird verwendet 929
Einzelheiten zur Richtlinie 929
Version der Richtlinie 930
JSON-Richtliniendokument 930
Weitere Informationen 930
AmazonMacieServiceRole 931
Diese Richtlinie wird verwendet 931
Einzelheiten zur Richtlinie 931
Version der Richtlinie 931
JSON-Richtliniendokument 931
Weitere Informationen 932
AmazonMacieServiceRolePolicy 932
Diese Richtlinie wird verwendet 932
Einzelheiten der Richtlinie 932
Version der Richtlinie 932
JSON-Richtliniendokument 933
Weitere Informationen 934
AmazonManagedBlockchainConsoleFullAccess 934
Diese Richtlinie wird verwendet 934
Einzelheiten zur Richtlinie 934
Version der Richtlinie 935
JSON-Richtliniendokument 935
Weitere Informationen 935
AmazonManagedBlockchainFullAccess 936
Diese Richtlinie wird verwendet 936
Einzelheiten zur Richtlinie 936
Version der Richtlinie 936
JSON-Richtliniendokument 936
Weitere Informationen 937

AmazonManagedBlockchainReadOnlyAccess 937
Diese Richtlinie wird verwendet 937
Einzelheiten zur Richtlinie 937
Version der Richtlinie 937
JSON-Richtliniendokument 938
Weitere Informationen 938
AmazonManagedBlockchainServiceRolePolicy 938
Diese Richtlinie wird verwendet 939
Einzelheiten der Richtlinie 939
Version der Richtlinie 939
JSON-Richtliniendokument 939
Weitere Informationen 940
AmazonMCSFullAccess 940
Diese Richtlinie wird verwendet 940
Einzelheiten zur Richtlinie 940
Version der Richtlinie 940
JSON-Richtliniendokument 941
Weitere Informationen 942
AmazonMCSReadOnlyAccess 942
Diese Richtlinie wird verwendet 942
Einzelheiten zur Richtlinie 942
Version der Richtlinie 943
JSON-Richtliniendokument 943
Weitere Informationen 943
AmazonMechanicalTurkFullAccess 944
Diese Richtlinie wird verwendet 944
Einzelheiten zur Richtlinie 944
Version der Richtlinie 944
JSON-Richtliniendokument 944
Weitere Informationen 945
AmazonMechanicalTurkReadOnly 945
Diese Richtlinie wird verwendet 945
Einzelheiten zur Richtlinie 945
Version der Richtlinie 945
JSON-Richtliniendokument 946
Weitere Informationen 946

AmazonMemoryDBFullAccess 946
Diese Richtlinie wird verwendet 946
Einzelheiten zur Richtlinie 947
Version der Richtlinie 947
JSON-Richtliniendokument 947
Weitere Informationen 948
AmazonMemoryDBReadOnlyAccess 948
Diese Richtlinie wird verwendet 948
Einzelheiten zur Richtlinie 948
Version der Richtlinie 948
JSON-Richtliniendokument 949
Weitere Informationen 949
AmazonMobileAnalyticsFinancialReportAccess 949
Diese Richtlinie wird verwendet 949
Einzelheiten zur Richtlinie 949
Version der Richtlinie 950
JSON-Richtliniendokument 950
Weitere Informationen 950
AmazonMobileAnalyticsFullAccess 951
Diese Richtlinie wird verwendet 951
Einzelheiten zur Richtlinie 951
Version der Richtlinie 951
JSON-Richtliniendokument 951
Weitere Informationen 952
AmazonMobileAnalyticsNon-financialReportAccess 952
Diese Richtlinie wird verwendet 952
Einzelheiten zur Richtlinie 952
Version der Richtlinie 952
JSON-Richtliniendokument 953
Weitere Informationen 953
AmazonMobileAnalyticsWriteOnlyAccess 953
Diese Richtlinie wird verwendet 953
Einzelheiten zur Richtlinie 953
Version der Richtlinie 954
JSON-Richtliniendokument 954
Weitere Informationen 954

AmazonMonitronFullAccess 954
Diese Richtlinie wird verwendet 955
Einzelheiten zur Richtlinie 955
Version der Richtlinie 955
JSON-Richtliniendokument 955
Weitere Informationen 957
AmazonMQApiFullAccess 957
Diese Richtlinie wird verwendet 957
Einzelheiten zur Richtlinie 957
Version der Richtlinie 958
JSON-Richtliniendokument 958
Weitere Informationen 959
AmazonMQApiReadOnlyAccess 959
Diese Richtlinie wird verwendet 959
Einzelheiten zur Richtlinie 959
Version der Richtlinie 960
JSON-Richtliniendokument 960
Weitere Informationen 960
AmazonMQFullAccess 961
Diese Richtlinie wird verwendet 961
Einzelheiten zur Richtlinie 961
Version der Richtlinie 961
JSON-Richtliniendokument 961
Weitere Informationen 962
AmazonMQReadOnlyAccess 963
Diese Richtlinie wird verwendet 963
Einzelheiten zur Richtlinie 963
Version der Richtlinie 963
JSON-Richtliniendokument 963
Weitere Informationen 964
AmazonMQServiceRolePolicy 964
Diese Richtlinie wird verwendet 964
Einzelheiten der Richtlinie 964
Version der Richtlinie 964
JSON-Richtliniendokument 965
Weitere Informationen 966

AmazonMSKConnectReadOnlyAccess 967
Diese Richtlinie wird verwendet 967
Einzelheiten zur Richtlinie 967
Version der Richtlinie 967
JSON-Richtliniendokument 967
Weitere Informationen 968
AmazonMSKFullAccess 969
Diese Richtlinie wird verwendet 969
Einzelheiten zur Richtlinie 969
Version der Richtlinie 969
JSON-Richtliniendokument 969
Weitere Informationen 972
AmazonMSKReadOnlyAccess 972
Diese Richtlinie wird verwendet 972
Einzelheiten zur Richtlinie 972
Version der Richtlinie 973
JSON-Richtliniendokument 973
Weitere Informationen 973
AmazonMWAAServerlessServiceRolePolicy 974
Diese Richtlinie wird verwendet 974
Einzelheiten der Richtlinie 974
Version der Richtlinie 974
JSON-Richtliniendokument 974
Weitere Informationen 975
AmazonMWAAServiceRolePolicy 975
Diese Richtlinie wird verwendet 975
Einzelheiten der Richtlinie 976
Version der Richtlinie 976
JSON-Richtliniendokument 976
Weitere Informationen 978
AmazonNimbleStudio-LaunchProfileWorker 978
Diese Richtlinie wird verwendet 979
Einzelheiten zur Richtlinie 979
Version der Richtlinie 979
JSON-Richtliniendokument 979
Weitere Informationen 980

AmazonNimbleStudio-StudioAdmin 980
Diese Richtlinie wird verwendet 980
Einzelheiten zur Richtlinie 980
Version der Richtlinie 980
JSON-Richtliniendokument 981
Weitere Informationen 983
AmazonNimbleStudio-StudioUser 983
Diese Richtlinie wird verwendet 983
Einzelheiten zur Richtlinie 983
Version der Richtlinie 983
JSON-Richtliniendokument 984
Weitere Informationen 986
AmazonODBServiceRolePolicy 986
Diese Richtlinie wird verwendet 986
Einzelheiten der Richtlinie 986
Version der Richtlinie 986
JSON-Richtliniendokument 987
Weitere Informationen 988
AmazonOmicsFullAccess 988
Diese Richtlinie wird verwendet 988
Einzelheiten zur Richtlinie 988
Version der Richtlinie 989
JSON-Richtliniendokument 989
Weitere Informationen 990
AmazonOmicsReadOnlyAccess 990
Diese Richtlinie wird verwendet 990
Einzelheiten zur Richtlinie 990
Version der Richtlinie 990
JSON-Richtliniendokument 991
Weitere Informationen 991
AmazonOneEnterpriseFullAccess 991
Diese Richtlinie wird verwendet 991
Einzelheiten zur Richtlinie 992
Version der Richtlinie 992
JSON-Richtliniendokument 992
Weitere Informationen 992

AmazonOneEnterpriseInstallerAccess 993
Diese Richtlinie wird verwendet 993
Einzelheiten zur Richtlinie 993
Version der Richtlinie 993
JSON-Richtliniendokument 993
Weitere Informationen 994
AmazonOneEnterpriseReadOnlyAccess 994
Diese Richtlinie wird verwendet 994
Einzelheiten zur Richtlinie 994
Version der Richtlinie 995
JSON-Richtliniendokument 995
Weitere Informationen 995
AmazonOpenSearchDashboardsServiceRolePolicy 996
Diese Richtlinie wird verwendet 996
Einzelheiten der Richtlinie 996
Version der Richtlinie 996
JSON-Richtliniendokument 996
Weitere Informationen 997
AmazonOpenSearchDirectQueryGlueCreateAccess 997
Diese Richtlinie wird verwendet 997
Einzelheiten zur Richtlinie 997
Version der Richtlinie 997
JSON-Richtliniendokument 998
Weitere Informationen 998
AmazonOpenSearchIngestionFullAccess 998
Diese Richtlinie wird verwendet 999
Einzelheiten zur Richtlinie 999
Version der Richtlinie 999
JSON-Richtliniendokument 999
Weitere Informationen 1000
AmazonOpenSearchIngestionReadOnlyAccess 1000
Diese Richtlinie wird verwendet 1000
Einzelheiten zur Richtlinie 1001
Version der Richtlinie 1001
JSON-Richtliniendokument 1001
Weitere Informationen 1001

AmazonOpenSearchIngestionServiceRolePolicy 1002
Diese Richtlinie wird verwendet 1002
Einzelheiten der Richtlinie 1002
Version der Richtlinie 1002
JSON-Richtliniendokument 1003
Weitere Informationen 1004
AmazonOpenSearchServerlessServiceRolePolicy 1005
Diese Richtlinie wird verwendet 1005
Einzelheiten der Richtlinie 1005
Version der Richtlinie 1005
JSON-Richtliniendokument 1005
Weitere Informationen 1006
AmazonOpenSearchServiceCognitoAccess 1006
Diese Richtlinie wird verwendet 1006
Einzelheiten zur Richtlinie 1006
Version der Richtlinie 1006
JSON-Richtliniendokument 1007
Weitere Informationen 1008
AmazonOpenSearchServiceFullAccess 1008
Diese Richtlinie wird verwendet 1008
Einzelheiten zur Richtlinie 1008
Version der Richtlinie 1008
JSON-Richtliniendokument 1009
Weitere Informationen 1009
AmazonOpenSearchServiceReadOnlyAccess 1009
Diese Richtlinie wird verwendet 1009
Einzelheiten zur Richtlinie 1010
Version der Richtlinie 1010
JSON-Richtliniendokument 1010
Weitere Informationen 1010
AmazonOpenSearchServiceRolePolicy 1011
Diese Richtlinie wird verwendet 1011
Einzelheiten der Richtlinie 1011
Version der Richtlinie 1011
JSON-Richtliniendokument 1011
Weitere Informationen 1016

AmazonPersonalizeFullAccess 1016
Diese Richtlinie wird verwendet 1017
Einzelheiten zur Richtlinie 1017
Version der Richtlinie 1017
JSON-Richtliniendokument 1017
Weitere Informationen 1018
AmazonPollyFullAccess 1018
Diese Richtlinie wird verwendet 1019
Einzelheiten zur Richtlinie 1019
Version der Richtlinie 1019
JSON-Richtliniendokument 1019
Weitere Informationen 1020
AmazonPollyReadOnlyAccess 1020
Diese Richtlinie wird verwendet 1020
Einzelheiten zur Richtlinie 1020
Version der Richtlinie 1020
JSON-Richtliniendokument 1020
Weitere Informationen 1021
AmazonPrometheusConsoleFullAccess 1021
Diese Richtlinie wird verwendet 1021
Einzelheiten zur Richtlinie 1022
Version der Richtlinie 1022
JSON-Richtliniendokument 1022
Weitere Informationen 1023
AmazonPrometheusFullAccess 1023
Diese Richtlinie wird verwendet 1024
Einzelheiten zur Richtlinie 1024
Version der Richtlinie 1024
JSON-Richtliniendokument 1024
Weitere Informationen 1025
AmazonPrometheusQueryAccess 1025
Diese Richtlinie wird verwendet 1026
Einzelheiten zur Richtlinie 1026
Version der Richtlinie 1026
JSON-Richtliniendokument 1026
Weitere Informationen 1027

AmazonPrometheusRemoteWriteAccess 1027
Diese Richtlinie wird verwendet 1027
Einzelheiten zur Richtlinie 1027
Version der Richtlinie 1027
JSON-Richtliniendokument 1028
Weitere Informationen 1028
AmazonPrometheusScraperServiceRolePolicy 1028
Diese Richtlinie wird verwendet 1028
Einzelheiten der Richtlinie 1028
Version der Richtlinie 1029
JSON-Richtliniendokument 1029
Weitere Informationen 1031
AmazonQDeveloperAccess 1031
Diese Richtlinie wird verwendet 1032
Einzelheiten zur Richtlinie 1032
Version der Richtlinie 1032
JSON-Richtliniendokument 1032
Weitere Informationen 1033
AmazonQFullAccess 1033
Diese Richtlinie wird verwendet 1034
Einzelheiten zur Richtlinie 1034
Version der Richtlinie 1034
JSON-Richtliniendokument 1034
Weitere Informationen 1036
AmazonQLDBConsoleFullAccess 1036
Diese Richtlinie wird verwendet 1036
Einzelheiten zur Richtlinie 1036
Version der Richtlinie 1036
JSON-Richtliniendokument 1037
Weitere Informationen 1038
AmazonQLDBFullAccess 1039
Diese Richtlinie wird verwendet 1039
Einzelheiten zur Richtlinie 1039
Version der Richtlinie 1039
JSON-Richtliniendokument 1039
Weitere Informationen 1041

AmazonQLDBReadOnly 1041
Diese Richtlinie wird verwendet 1041
Einzelheiten zur Richtlinie 1041
Version der Richtlinie 1041
JSON-Richtliniendokument 1042
Weitere Informationen 1042
AmazonRDSBetaServiceRolePolicy 1042
Diese Richtlinie wird verwendet 1043
Einzelheiten der Richtlinie 1043
Version der Richtlinie 1043
JSON-Richtliniendokument 1043
Weitere Informationen 1046
AmazonRDSCustomInstanceProfileRolePolicy 1046
Diese Richtlinie wird verwendet 1046
Einzelheiten zur Richtlinie 1047
Version der Richtlinie 1047
JSON-Richtliniendokument 1047
Weitere Informationen 1054
AmazonRDSCustomPreviewServiceRolePolicy 1054
Diese Richtlinie wird verwendet 1055
Einzelheiten der Richtlinie 1055
Version der Richtlinie 1055
JSON-Richtliniendokument 1055
Weitere Informationen 1073
AmazonRDSCustomServiceRolePolicy 1073
Diese Richtlinie wird verwendet 1073
Einzelheiten der Richtlinie 1073
Version der Richtlinie 1073
JSON-Richtliniendokument 1074
Weitere Informationen 1093
AmazonRDSDataFullAccess 1093
Diese Richtlinie wird verwendet 1093
Einzelheiten zur Richtlinie 1093
Version der Richtlinie 1093
JSON-Richtliniendokument 1094
Weitere Informationen 1095

AmazonRDSDirectoryServiceAccess 1095
Diese Richtlinie wird verwendet 1095
Einzelheiten zur Richtlinie 1095
Version der Richtlinie 1095
JSON-Richtliniendokument 1096
Weitere Informationen 1096
AmazonRDSEnhancedMonitoringRole 1096
Diese Richtlinie wird verwendet 1096
Einzelheiten zur Richtlinie 1097
Version der Richtlinie 1097
JSON-Richtliniendokument 1097
Weitere Informationen 1098
AmazonRDSFullAccess 1098
Diese Richtlinie wird verwendet 1098
Einzelheiten zur Richtlinie 1098
Version der Richtlinie 1098
JSON-Richtliniendokument 1099
Weitere Informationen 1101
AmazonRDSPerformanceInsightsFullAccess 1101
Diese Richtlinie wird verwendet 1101
Einzelheiten zur Richtlinie 1101
Version der Richtlinie 1101
JSON-Richtliniendokument 1102
Weitere Informationen 1103
AmazonRDSPerformanceInsightsReadOnly 1103
Diese Richtlinie wird verwendet 1104
Einzelheiten zur Richtlinie 1104
Version der Richtlinie 1104
JSON-Richtliniendokument 1104
Weitere Informationen 1106
AmazonRDSPreviewServiceRolePolicy 1106
Diese Richtlinie wird verwendet 1107
Einzelheiten der Richtlinie 1107
Version der Richtlinie 1107
JSON-Richtliniendokument 1107
Weitere Informationen 1110

AmazonRDSReadOnlyAccess 1110
Diese Richtlinie wird verwendet 1111
Einzelheiten zur Richtlinie 1111
Version der Richtlinie 1111
JSON-Richtliniendokument 1111
Weitere Informationen 1112
AmazonRDSServiceRolePolicy 1113
Diese Richtlinie wird verwendet 1113
Einzelheiten der Richtlinie 1113
Version der Richtlinie 1113
JSON-Richtliniendokument 1113
Weitere Informationen 1117
AmazonRedshiftAllCommandsFullAccess 1117
Diese Richtlinie wird verwendet 1117
Einzelheiten zur Richtlinie 1118
Version der Richtlinie 1118
JSON-Richtliniendokument 1118
Weitere Informationen 1123
AmazonRedshiftDataFullAccess 1123
Diese Richtlinie wird verwendet 1124
Einzelheiten zur Richtlinie 1124
Version der Richtlinie 1124
JSON-Richtliniendokument 1124
Weitere Informationen 1126
AmazonRedshiftFederatedAuthorization 1126
Diese Richtlinie wird verwendet 1127
Einzelheiten zur Richtlinie 1127
Version der Richtlinie 1127
JSON-Richtliniendokument 1127
Weitere Informationen 1128
AmazonRedshiftFullAccess 1128
Diese Richtlinie wird verwendet 1129
Einzelheiten zur Richtlinie 1129
Version der Richtlinie 1129
JSON-Richtliniendokument 1129
Weitere Informationen 1131

AmazonRedshiftQueryEditor 1131
Diese Richtlinie wird verwendet 1132
Einzelheiten zur Richtlinie 1132
Version der Richtlinie 1132
JSON-Richtliniendokument 1132
Weitere Informationen 1134
AmazonRedshiftQueryEditorV2FullAccess 1134
Diese Richtlinie wird verwendet 1134
Einzelheiten zur Richtlinie 1135
Version der Richtlinie 1135
JSON-Richtliniendokument 1135
Weitere Informationen 1136
AmazonRedshiftQueryEditorV2NoSharing 1137
Diese Richtlinie wird verwendet 1137
Einzelheiten zur Richtlinie 1137
Version der Richtlinie 1137
JSON-Richtliniendokument 1137
Weitere Informationen 1141
AmazonRedshiftQueryEditorV2ReadSharing 1141
Diese Richtlinie wird verwendet 1142
Einzelheiten zur Richtlinie 1142
Version der Richtlinie 1142
JSON-Richtliniendokument 1142
Weitere Informationen 1147
AmazonRedshiftQueryEditorV2ReadWriteSharing 1147
Diese Richtlinie wird verwendet 1148
Einzelheiten zur Richtlinie 1148
Version der Richtlinie 1148
JSON-Richtliniendokument 1148
Weitere Informationen 1153
AmazonRedshiftReadOnlyAccess 1153
Diese Richtlinie wird verwendet 1153
Einzelheiten zur Richtlinie 1154
Version der Richtlinie 1154
JSON-Richtliniendokument 1154
Weitere Informationen 1155

AmazonRedshiftServiceLinkedRolePolicy 1155
Diese Richtlinie wird verwendet 1155
Einzelheiten der Richtlinie 1155
Version der Richtlinie 1155
JSON-Richtliniendokument 1156
Weitere Informationen 1162
AmazonRekognitionCustomLabelsFullAccess 1162
Diese Richtlinie wird verwendet 1162
Einzelheiten zur Richtlinie 1162
Version der Richtlinie 1163
JSON-Richtliniendokument 1163
Weitere Informationen 1164
AmazonRekognitionFullAccess 1164
Diese Richtlinie wird verwendet 1164
Einzelheiten zur Richtlinie 1165
Version der Richtlinie 1165
JSON-Richtliniendokument 1165
Weitere Informationen 1165
AmazonRekognitionReadOnlyAccess 1166
Diese Richtlinie wird verwendet 1166
Einzelheiten zur Richtlinie 1166
Version der Richtlinie 1166
JSON-Richtliniendokument 1166
Weitere Informationen 1167
AmazonRekognitionServiceRole 1168
Diese Richtlinie wird verwendet 1168
Einzelheiten zur Richtlinie 1168
Version der Richtlinie 1168
JSON-Richtliniendokument 1168
Weitere Informationen 1169
AmazonRoute53AutoNamingFullAccess 1169
Diese Richtlinie wird verwendet 1170
Einzelheiten zur Richtlinie 1170
Version der Richtlinie 1170
JSON-Richtliniendokument 1170
Weitere Informationen 1171

AmazonRoute53AutoNamingReadOnlyAccess 1171
Diese Richtlinie wird verwendet 1171
Einzelheiten zur Richtlinie 1171
Version der Richtlinie 1172
JSON-Richtliniendokument 1172
Weitere Informationen 1172
AmazonRoute53AutoNamingRegistrantAccess 1172
Diese Richtlinie wird verwendet 1173
Einzelheiten zur Richtlinie 1173
Version der Richtlinie 1173
JSON-Richtliniendokument 1173
Weitere Informationen 1174
AmazonRoute53DomainsFullAccess 1174
Diese Richtlinie wird verwendet 1174
Einzelheiten zur Richtlinie 1174
Version der Richtlinie 1175
JSON-Richtliniendokument 1175
Weitere Informationen 1175
AmazonRoute53DomainsReadOnlyAccess 1175
Diese Richtlinie wird verwendet 1176
Einzelheiten zur Richtlinie 1176
Version der Richtlinie 1176
JSON-Richtliniendokument 1176
Weitere Informationen 1177
AmazonRoute53FullAccess 1177
Diese Richtlinie wird verwendet 1177
Einzelheiten zur Richtlinie 1177
Version der Richtlinie 1177
JSON-Richtliniendokument 1178
Weitere Informationen 1179
AmazonRoute53ProfilesFullAccess 1179
Diese Richtlinie wird verwendet 1179
Einzelheiten zur Richtlinie 1179
Version der Richtlinie 1179
JSON-Richtliniendokument 1180
Weitere Informationen 1181

AmazonRoute53ProfilesReadOnlyAccess 1181
Diese Richtlinie wird verwendet 1181
Einzelheiten zur Richtlinie 1181
Version der Richtlinie 1181
JSON-Richtliniendokument 1182
Weitere Informationen 1182
AmazonRoute53ReadOnlyAccess 1183
Diese Richtlinie wird verwendet 1183
Einzelheiten zur Richtlinie 1183
Version der Richtlinie 1183
JSON-Richtliniendokument 1183
Weitere Informationen 1184
AmazonRoute53RecoveryClusterFullAccess 1184
Diese Richtlinie wird verwendet 1184
Einzelheiten zur Richtlinie 1184
Version der Richtlinie 1184
JSON-Richtliniendokument 1185
Weitere Informationen 1185
AmazonRoute53RecoveryClusterReadOnlyAccess 1185
Diese Richtlinie wird verwendet 1185
Einzelheiten zur Richtlinie 1186
Version der Richtlinie 1186
JSON-Richtliniendokument 1186
Weitere Informationen 1186
AmazonRoute53RecoveryControlConfigFullAccess 1187
Diese Richtlinie wird verwendet 1187
Einzelheiten zur Richtlinie 1187
Version der Richtlinie 1187
JSON-Richtliniendokument 1187
Weitere Informationen 1188
AmazonRoute53RecoveryControlConfigReadOnlyAccess 1188
Diese Richtlinie wird verwendet 1188
Einzelheiten zur Richtlinie 1188
Version der Richtlinie 1188
JSON-Richtliniendokument 1189
Weitere Informationen 1189

AmazonRoute53RecoveryReadinessFullAccess 1190
Diese Richtlinie wird verwendet 1190
Einzelheiten zur Richtlinie 1190
Version der Richtlinie 1190
JSON-Richtliniendokument 1190
Weitere Informationen 1191
AmazonRoute53RecoveryReadinessReadOnlyAccess 1191
Diese Richtlinie wird verwendet 1191
Einzelheiten zur Richtlinie 1191
Version der Richtlinie 1191
JSON-Richtliniendokument 1192
Weitere Informationen 1192
AmazonRoute53ResolverFullAccess 1193
Diese Richtlinie wird verwendet 1193
Einzelheiten zur Richtlinie 1193
Version der Richtlinie 1193
JSON-Richtliniendokument 1193
Weitere Informationen 1194
AmazonRoute53ResolverReadOnlyAccess 1194
Diese Richtlinie wird verwendet 1194
Einzelheiten zur Richtlinie 1195
Version der Richtlinie 1195
JSON-Richtliniendokument 1195
Weitere Informationen 1196
AmazonS3FullAccess 1196
Diese Richtlinie wird verwendet 1196
Einzelheiten zur Richtlinie 1196
Version der Richtlinie 1196
JSON-Richtliniendokument 1196
Weitere Informationen 1197
AmazonS3ObjectLambdaExecutionRolePolicy 1197
Diese Richtlinie wird verwendet 1197
Einzelheiten zur Richtlinie 1197
Version der Richtlinie 1198
JSON-Richtliniendokument 1198
Weitere Informationen 1198

AmazonS3OutpostsFullAccess 1199
Diese Richtlinie wird verwendet 1199
Einzelheiten zur Richtlinie 1199
Version der Richtlinie 1199
JSON-Richtliniendokument 1199
Weitere Informationen 1200
AmazonS3OutpostsReadOnlyAccess 1200
Diese Richtlinie wird verwendet 1201
Einzelheiten zur Richtlinie 1201
Version der Richtlinie 1201
JSON-Richtliniendokument 1201
Weitere Informationen 1202
AmazonS3ReadOnlyAccess 1202
Diese Richtlinie wird verwendet 1203
Einzelheiten zur Richtlinie 1203
Version der Richtlinie 1203
JSON-Richtliniendokument 1203
Weitere Informationen 1204
AmazonS3TablesFullAccess 1204
Diese Richtlinie wird verwendet 1204
Einzelheiten zur Richtlinie 1204
Version der Richtlinie 1204
JSON-Richtliniendokument 1204
Weitere Informationen 1205
AmazonS3TablesLakeFormationServiceRole 1205
Diese Richtlinie wird verwendet 1206
Einzelheiten zur Richtlinie 1206
Version der Richtlinie 1206
JSON-Richtliniendokument 1206
Weitere Informationen 1208
AmazonS3TablesReadOnlyAccess 1209
Diese Richtlinie wird verwendet 1209
Einzelheiten zur Richtlinie 1209
Version der Richtlinie 1209
JSON-Richtliniendokument 1209
Weitere Informationen 1210

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy 1210
Diese Richtlinie wird verwendet 1210
Einzelheiten zur Richtlinie 1210
Version der Richtlinie 1211
JSON-Richtliniendokument 1211
Weitere Informationen 1222
AmazonSageMakerCanvasAIServicesAccess 1222
Diese Richtlinie wird verwendet 1223
Einzelheiten zur Richtlinie 1223
Version der Richtlinie 1223
JSON-Richtliniendokument 1223
Weitere Informationen 1226
AmazonSageMakerCanvasBedrockAccess 1226
Diese Richtlinie wird verwendet 1227
Einzelheiten zur Richtlinie 1227
Version der Richtlinie 1227
JSON-Richtliniendokument 1227
Weitere Informationen 1228
AmazonSageMakerCanvasDataPrepFullAccess 1228
Diese Richtlinie wird verwendet 1228
Einzelheiten zur Richtlinie 1228
Version der Richtlinie 1229
JSON-Richtliniendokument 1229
Weitere Informationen 1238
AmazonSageMakerCanvasDirectDeployAccess 1239
Diese Richtlinie wird verwendet 1239
Einzelheiten zur Richtlinie 1239
Version der Richtlinie 1239
JSON-Richtliniendokument 1239
Weitere Informationen 1240
AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy 1240
Diese Richtlinie wird verwendet 1241
Einzelheiten zur Richtlinie 1241
Version der Richtlinie 1241
JSON-Richtliniendokument 1241
Weitere Informationen 1242

AmazonSageMakerCanvasForecastAccess 1243
Diese Richtlinie wird verwendet 1243
Einzelheiten zur Richtlinie 1243
Version der Richtlinie 1243
JSON-Richtliniendokument 1243
Weitere Informationen 1244
AmazonSageMakerCanvasFullAccess 1244
Diese Richtlinie wird verwendet 1245
Einzelheiten zur Richtlinie 1245
Version der Richtlinie 1245
JSON-Richtliniendokument 1245
Weitere Informationen 1257
AmazonSageMakerCanvasSMDataScienceAssistantAccess 1258
Diese Richtlinie wird verwendet 1258
Einzelheiten zur Richtlinie 1258
Version der Richtlinie 1258
JSON-Richtliniendokument 1258
Weitere Informationen 1259
AmazonSageMakerClusterInstanceRolePolicy 1259
Diese Richtlinie wird verwendet 1260
Einzelheiten zur Richtlinie 1260
Version der Richtlinie 1260
JSON-Richtliniendokument 1260
Weitere Informationen 1262
AmazonSageMakerCoreServiceRolePolicy 1262
Diese Richtlinie wird verwendet 1262
Einzelheiten der Richtlinie 1262
Version der Richtlinie 1263
JSON-Richtliniendokument 1263
Weitere Informationen 1264
AmazonSageMakerEdgeDeviceFleetPolicy 1264
Diese Richtlinie wird verwendet 1264
Einzelheiten zur Richtlinie 1264
Version der Richtlinie 1264
JSON-Richtliniendokument 1265
Weitere Informationen 1266

AmazonSageMakerFeatureStoreAccess 1267
Diese Richtlinie wird verwendet 1267
Einzelheiten zur Richtlinie 1267
Version der Richtlinie 1267
JSON-Richtliniendokument 1267
Weitere Informationen 1268
AmazonSageMakerFullAccess 1269
Diese Richtlinie wird verwendet 1269
Einzelheiten zur Richtlinie 1269
Version der Richtlinie 1269
JSON-Richtliniendokument 1269
Weitere Informationen 1286
AmazonSageMakerGeospatialExecutionRole 1286
Diese Richtlinie wird verwendet 1286
Einzelheiten zur Richtlinie 1286
Version der Richtlinie 1286
JSON-Richtliniendokument 1287
Weitere Informationen 1287
AmazonSageMakerGeospatialFullAccess 1288
Diese Richtlinie wird verwendet 1288
Einzelheiten zur Richtlinie 1288
Version der Richtlinie 1288
JSON-Richtliniendokument 1288
Weitere Informationen 1289
AmazonSageMakerGroundTruthExecution 1289
Diese Richtlinie wird verwendet 1290
Einzelheiten zur Richtlinie 1290
Version der Richtlinie 1290
JSON-Richtliniendokument 1290
Weitere Informationen 1294
AmazonSageMakerHyperPodObservabilityAdminAccess 1294
Diese Richtlinie wird verwendet 1294
Einzelheiten zur Richtlinie 1294
Version der Richtlinie 1294
JSON-Richtliniendokument 1295
Weitere Informationen 1301

AmazonSageMakerHyperPodServiceRolePolicy 1301
Diese Richtlinie wird verwendet 1301
Einzelheiten der Richtlinie 1301
Version der Richtlinie 1302
JSON-Richtliniendokument 1302
Weitere Informationen 1303
AmazonSageMakerHyperPodTrainingOperatorAccess 1303
Diese Richtlinie wird verwendet 1303
Einzelheiten zur Richtlinie 1303
Version der Richtlinie 1304
JSON-Richtliniendokument 1304
Weitere Informationen 1304
AmazonSageMakerMechanicalTurkAccess 1305
Diese Richtlinie wird verwendet 1305
Einzelheiten zur Richtlinie 1305
Version der Richtlinie 1305
JSON-Richtliniendokument 1305
Weitere Informationen 1306
AmazonSageMakerModelGovernanceUseAccess 1306
Diese Richtlinie wird verwendet 1306
Einzelheiten zur Richtlinie 1306
Version der Richtlinie 1306
JSON-Richtliniendokument 1307
Weitere Informationen 1309
AmazonSageMakerModelRegistryFullAccess 1309
Diese Richtlinie wird verwendet 1309
Einzelheiten zur Richtlinie 1309
Version der Richtlinie 1309
JSON-Richtliniendokument 1310
Weitere Informationen 1313
AmazonSageMakerNotebooksServiceRolePolicy 1313
Diese Richtlinie wird verwendet 1314
Einzelheiten der Richtlinie 1314
Version der Richtlinie 1314
JSON-Richtliniendokument 1314
Weitere Informationen 1319

AmazonSageMakerPartnerAppsFullAccess 1320
Diese Richtlinie wird verwendet 1320
Einzelheiten zur Richtlinie 1320
Version der Richtlinie 1320
JSON-Richtliniendokument 1320
Weitere Informationen 1321
AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy 1321
Diese Richtlinie wird verwendet 1322
Einzelheiten zur Richtlinie 1322
Version der Richtlinie 1322
JSON-Richtliniendokument 1322
Weitere Informationen 1323
AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy 1323
Diese Richtlinie wird verwendet 1324
Einzelheiten zur Richtlinie 1324
Version der Richtlinie 1324
JSON-Richtliniendokument 1324
Weitere Informationen 1328
AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy 1328
Diese Richtlinie wird verwendet 1328
Einzelheiten zur Richtlinie 1328
Version der Richtlinie 1328
JSON-Richtliniendokument 1329
Weitere Informationen 1329
AmazonSageMakerPipelinesIntegrations 1329
Diese Richtlinie wird verwendet 1330
Einzelheiten zur Richtlinie 1330
Version der Richtlinie 1330
JSON-Richtliniendokument 1330
Weitere Informationen 1332
AmazonSageMakerQuickSightVPCPolicy 1332
Diese Richtlinie wird verwendet 1332
Einzelheiten zur Richtlinie 1332
Version der Richtlinie 1333
JSON-Richtliniendokument 1333
Weitere Informationen 1334

AmazonSageMakerReadOnly 1335
Diese Richtlinie wird verwendet 1335
Einzelheiten zur Richtlinie 1335
Version der Richtlinie 1335
JSON-Richtliniendokument 1335
Weitere Informationen 1336
AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy 1337
Diese Richtlinie wird verwendet 1337
Einzelheiten zur Richtlinie 1337
Version der Richtlinie 1337
JSON-Richtliniendokument 1338
Weitere Informationen 1338
AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy 1339
Diese Richtlinie wird verwendet 1339
Einzelheiten zur Richtlinie 1339
Version der Richtlinie 1339
JSON-Richtliniendokument 1339
Weitere Informationen 1346
AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy 1346
Diese Richtlinie wird verwendet 1347
Einzelheiten zur Richtlinie 1347
Version der Richtlinie 1347
JSON-Richtliniendokument 1347
Weitere Informationen 1357
AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy 1358
Diese Richtlinie wird verwendet 1358
Einzelheiten zur Richtlinie 1358
Version der Richtlinie 1358
JSON-Richtliniendokument 1358
Weitere Informationen 1361
AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy 1361
Diese Richtlinie wird verwendet 1362
Einzelheiten zur Richtlinie 1362
Version der Richtlinie 1362
JSON-Richtliniendokument 1362
Weitere Informationen 1363

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy 1363
Diese Richtlinie wird verwendet 1363
Einzelheiten zur Richtlinie 1363
Version der Richtlinie 1363
JSON-Richtliniendokument 1364
Weitere Informationen 1364
AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy 1364
Diese Richtlinie wird verwendet 1365
Einzelheiten zur Richtlinie 1365
Version der Richtlinie 1365
JSON-Richtliniendokument 1365
Weitere Informationen 1367
AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy 1368
Diese Richtlinie wird verwendet 1368
Einzelheiten zur Richtlinie 1368
Version der Richtlinie 1368
JSON-Richtliniendokument 1368
Weitere Informationen 1378
AmazonSageMakerSpacesControllerPolicy 1379
Diese Richtlinie wird verwendet 1379
Einzelheiten zur Richtlinie 1379
Version der Richtlinie 1379
JSON-Richtliniendokument 1379
Weitere Informationen 1384
AmazonSageMakerSpacesRouterPolicy 1384
Diese Richtlinie wird verwendet 1384
Einzelheiten zur Richtlinie 1384
Version der Richtlinie 1385
JSON-Richtliniendokument 1385
Weitere Informationen 1386
AmazonSageMakerTrainingPlanCreateAccess 1386
Diese Richtlinie wird verwendet 1386
Einzelheiten zur Richtlinie 1386
Version der Richtlinie 1386
JSON-Richtliniendokument 1387
Weitere Informationen 1388

AmazonSecurityLakeAdministrator 1388
Diese Richtlinie wird verwendet 1389
Einzelheiten zur Richtlinie 1389
Version der Richtlinie 1389
JSON-Richtliniendokument 1389
Weitere Informationen 1400
AmazonSecurityLakeMetastoreManager 1401
Diese Richtlinie wird verwendet 1401
Einzelheiten zur Richtlinie 1401
Version der Richtlinie 1401
JSON-Richtliniendokument 1401
Weitere Informationen 1404
AmazonSecurityLakePermissionsBoundary 1404
Diese Richtlinie wird verwendet 1404
Einzelheiten zur Richtlinie 1404
Version der Richtlinie 1404
JSON-Richtliniendokument 1405
Weitere Informationen 1408
AmazonSESFullAccess 1408
Diese Richtlinie wird verwendet 1408
Einzelheiten zur Richtlinie 1408
Version der Richtlinie 1408
JSON-Richtliniendokument 1409
Weitere Informationen 1409
AmazonSESReadOnlyAccess 1409
Diese Richtlinie wird verwendet 1409
Einzelheiten zur Richtlinie 1410
Version der Richtlinie 1410
JSON-Richtliniendokument 1410
Weitere Informationen 1410
AmazonSESServiceRolePolicy 1411
Diese Richtlinie wird verwendet 1411
Einzelheiten der Richtlinie 1411
Version der Richtlinie 1411
JSON-Richtliniendokument 1411
Weitere Informationen 1412

AmazonSNSFullAccess 1412
Diese Richtlinie wird verwendet 1412
Einzelheiten zur Richtlinie 1412
Version der Richtlinie 1413
JSON-Richtliniendokument 1413
Weitere Informationen 1414
AmazonSNSReadOnlyAccess 1414
Diese Richtlinie wird verwendet 1414
Einzelheiten zur Richtlinie 1414
Version der Richtlinie 1414
JSON-Richtliniendokument 1415
Weitere Informationen 1416
AmazonSNSRole 1416
Diese Richtlinie wird verwendet 1416
Einzelheiten zur Richtlinie 1416
Version der Richtlinie 1416
JSON-Richtliniendokument 1417
Weitere Informationen 1417
AmazonSQSFullAccess 1417
Diese Richtlinie wird verwendet 1417
Einzelheiten zur Richtlinie 1418
Version der Richtlinie 1418
JSON-Richtliniendokument 1418
Weitere Informationen 1418
AmazonSQSReadOnlyAccess 1419
Diese Richtlinie wird verwendet 1419
Einzelheiten zur Richtlinie 1419
Version der Richtlinie 1419
JSON-Richtliniendokument 1419
Weitere Informationen 1420
AmazonSSMAutomationApproverAccess 1420
Diese Richtlinie wird verwendet 1420
Einzelheiten zur Richtlinie 1420
Version der Richtlinie 1421
JSON-Richtliniendokument 1421
Weitere Informationen 1421

AmazonSSMAutomationRole 1422
Diese Richtlinie wird verwendet 1422
Einzelheiten zur Richtlinie 1422
Version der Richtlinie 1422
JSON-Richtliniendokument 1422
Weitere Informationen 1424
AmazonSSMDirectoryServiceAccess 1424
Diese Richtlinie wird verwendet 1424
Einzelheiten zur Richtlinie 1424
Version der Richtlinie 1425
JSON-Richtliniendokument 1425
Weitere Informationen 1425
AmazonSSMFullAccess 1425
Diese Richtlinie wird verwendet 1426
Einzelheiten zur Richtlinie 1426
Version der Richtlinie 1426
JSON-Richtliniendokument 1426
Weitere Informationen 1427
AmazonSSMMaintenanceWindowRole 1428
Diese Richtlinie wird verwendet 1428
Einzelheiten zur Richtlinie 1428
Version der Richtlinie 1428
JSON-Richtliniendokument 1428
Weitere Informationen 1430
AmazonSSMManagedEC2InstanceDefaultPolicy 1430
Diese Richtlinie wird verwendet 1430
Einzelheiten zur Richtlinie 1430
Version der Richtlinie 1430
JSON-Richtliniendokument 1431
Weitere Informationen 1432
AmazonSSMManagedInstanceCore 1432
Diese Richtlinie wird verwendet 1432
Einzelheiten zur Richtlinie 1432
Version der Richtlinie 1433
JSON-Richtliniendokument 1433
Weitere Informationen 1434

AmazonSSMPatchAssociation 1434
Diese Richtlinie wird verwendet 1434
Einzelheiten zur Richtlinie 1434
Version der Richtlinie 1435
JSON-Richtliniendokument 1435
Weitere Informationen 1436
AmazonSSMReadOnlyAccess 1436
Diese Richtlinie wird verwendet 1436
Einzelheiten zur Richtlinie 1436
Version der Richtlinie 1436
JSON-Richtliniendokument 1436
Weitere Informationen 1437
AmazonSSMServiceRolePolicy 1437
Diese Richtlinie wird verwendet 1437
Einzelheiten der Richtlinie 1437
Version der Richtlinie 1438
JSON-Richtliniendokument 1438
Weitere Informationen 1443
AmazonSumerianFullAccess 1444
Diese Richtlinie wird verwendet 1444
Einzelheiten zur Richtlinie 1444
Version der Richtlinie 1444
JSON-Richtliniendokument 1444
Weitere Informationen 1445
AmazonTextractFullAccess 1445
Diese Richtlinie wird verwendet 1445
Einzelheiten zur Richtlinie 1445
Version der Richtlinie 1445
JSON-Richtliniendokument 1446
Weitere Informationen 1446
AmazonTextractServiceRole 1446
Diese Richtlinie wird verwendet 1446
Einzelheiten zur Richtlinie 1446
Version der Richtlinie 1447
JSON-Richtliniendokument 1447
Weitere Informationen 1447

AmazonTimestreamConsoleFullAccess 1448
Diese Richtlinie wird verwendet 1448
Einzelheiten zur Richtlinie 1448
Version der Richtlinie 1448
JSON-Richtliniendokument 1448
Weitere Informationen 1451
AmazonTimestreamFullAccess 1451
Diese Richtlinie wird verwendet 1451
Einzelheiten zur Richtlinie 1452
Version der Richtlinie 1452
JSON-Richtliniendokument 1452
Weitere Informationen 1453
AmazonTimestreamInfluxDBFullAccess 1453
Diese Richtlinie wird verwendet 1454
Einzelheiten zur Richtlinie 1454
Version der Richtlinie 1454
JSON-Richtliniendokument 1454
Weitere Informationen 1457
AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess 1457
Diese Richtlinie wird verwendet 1457
Einzelheiten zur Richtlinie 1457
Version der Richtlinie 1457
JSON-Richtliniendokument 1458
Weitere Informationen 1460
AmazonTimestreamInfluxDBServiceRolePolicy 1460
Diese Richtlinie wird verwendet 1460
Einzelheiten der Richtlinie 1460
Version der Richtlinie 1461
JSON-Richtliniendokument 1461
Weitere Informationen 1463
AmazonTimestreamReadOnlyAccess 1463
Diese Richtlinie wird verwendet 1464
Einzelheiten zur Richtlinie 1464
Version der Richtlinie 1464
JSON-Richtliniendokument 1464
Weitere Informationen 1465

AmazonTranscribeFullAccess 1465
Diese Richtlinie wird verwendet 1465
Einzelheiten zur Richtlinie 1465
Version der Richtlinie 1466
JSON-Richtliniendokument 1466
Weitere Informationen 1466
AmazonTranscribeReadOnlyAccess 1467
Diese Richtlinie wird verwendet 1467
Einzelheiten zur Richtlinie 1467
Version der Richtlinie 1467
JSON-Richtliniendokument 1467
Weitere Informationen 1468
AmazonVerifiedPermissionsFullAccess 1468
Diese Richtlinie wird verwendet 1468
Einzelheiten zur Richtlinie 1468
Version der Richtlinie 1468
JSON-Richtliniendokument 1469
Weitere Informationen 1469
AmazonVerifiedPermissionsReadOnlyAccess 1469
Diese Richtlinie wird verwendet 1470
Einzelheiten zur Richtlinie 1470
Version der Richtlinie 1470
JSON-Richtliniendokument 1470
Weitere Informationen 1471
AmazonVPCCrossAccountNetworkInterfaceOperations 1471
Diese Richtlinie wird verwendet 1471
Einzelheiten zur Richtlinie 1471
Version der Richtlinie 1472
JSON-Richtliniendokument 1472
Weitere Informationen 1473
AmazonVPCFullAccess 1474
Diese Richtlinie wird verwendet 1474
Einzelheiten zur Richtlinie 1474
Version der Richtlinie 1474
JSON-Richtliniendokument 1474
Weitere Informationen 1478

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy 1478
Diese Richtlinie wird verwendet 1479
Einzelheiten zur Richtlinie 1479
Version der Richtlinie 1479
JSON-Richtliniendokument 1479
Weitere Informationen 1482
AmazonVPCReachabilityAnalyzerFullAccessPolicy 1483
Diese Richtlinie wird verwendet 1483
Einzelheiten zur Richtlinie 1483
Version der Richtlinie 1483
JSON-Richtliniendokument 1483
Weitere Informationen 1486
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy 1487
Diese Richtlinie wird verwendet 1487
Einzelheiten zur Richtlinie 1487
Version der Richtlinie 1487
JSON-Richtliniendokument 1488
Weitere Informationen 1488
AmazonVPCReadOnlyAccess 1488
Diese Richtlinie wird verwendet 1488
Einzelheiten zur Richtlinie 1488
Version der Richtlinie 1489
JSON-Richtliniendokument 1489
Weitere Informationen 1490
AmazonWorkDocsFullAccess 1490
Diese Richtlinie wird verwendet 1491
Einzelheiten zur Richtlinie 1491
Version der Richtlinie 1491
JSON-Richtliniendokument 1491
Weitere Informationen 1492
AmazonWorkDocsReadOnlyAccess 1492
Diese Richtlinie wird verwendet 1492
Einzelheiten zur Richtlinie 1492
Version der Richtlinie 1492
JSON-Richtliniendokument 1492
Weitere Informationen 1493

AmazonWorkMailEventsServiceRolePolicy 1493
Diese Richtlinie wird verwendet 1493
Einzelheiten der Richtlinie 1493
Version der Richtlinie 1494
JSON-Richtliniendokument 1494
Weitere Informationen 1494
AmazonWorkMailFullAccess 1495
Diese Richtlinie wird verwendet 1495
Einzelheiten zur Richtlinie 1495
Version der Richtlinie 1495
JSON-Richtliniendokument 1495
Weitere Informationen 1497
AmazonWorkMailMessageFlowFullAccess 1497
Diese Richtlinie wird verwendet 1498
Einzelheiten zur Richtlinie 1498
Version der Richtlinie 1498
JSON-Richtliniendokument 1498
Weitere Informationen 1499
AmazonWorkMailMessageFlowReadOnlyAccess 1499
Diese Richtlinie wird verwendet 1499
Einzelheiten zur Richtlinie 1499
Version der Richtlinie 1499
JSON-Richtliniendokument 1500
Weitere Informationen 1500
AmazonWorkMailReadOnlyAccess 1500
Diese Richtlinie wird verwendet 1500
Einzelheiten zur Richtlinie 1500
Version der Richtlinie 1501
JSON-Richtliniendokument 1501
Weitere Informationen 1501
AmazonWorkSpacesAdmin 1502
Diese Richtlinie wird verwendet 1502
Einzelheiten zur Richtlinie 1502
Version der Richtlinie 1502
JSON-Richtliniendokument 1502
Weitere Informationen 1503

AmazonWorkSpacesApplicationManagerAdminAccess 1504
Diese Richtlinie wird verwendet 1504
Einzelheiten zur Richtlinie 1504
Version der Richtlinie 1504
JSON-Richtliniendokument 1504
Weitere Informationen 1505
AmazonWorkspacesPCAAccess 1505
Diese Richtlinie wird verwendet 1505
Einzelheiten zur Richtlinie 1505
Version der Richtlinie 1505
JSON-Richtliniendokument 1506
Weitere Informationen 1506
AmazonWorkSpacesPoolServiceAccess 1506
Diese Richtlinie wird verwendet 1507
Einzelheiten zur Richtlinie 1507
Version der Richtlinie 1507
JSON-Richtliniendokument 1507
Weitere Informationen 1508
AmazonWorkSpacesSecureBrowserReadOnly 1509
Diese Richtlinie wird verwendet 1509
Einzelheiten zur Richtlinie 1509
Version der Richtlinie 1509
JSON-Richtliniendokument 1509
Weitere Informationen 1510
AmazonWorkSpacesSelfServiceAccess 1511
Diese Richtlinie wird verwendet 1511
Einzelheiten zur Richtlinie 1511
Version der Richtlinie 1511
JSON-Richtliniendokument 1511
Weitere Informationen 1512
AmazonWorkSpacesServiceAccess 1512
Diese Richtlinie wird verwendet 1512
Einzelheiten zur Richtlinie 1512
Version der Richtlinie 1512
JSON-Richtliniendokument 1513
Weitere Informationen 1513

AmazonWorkSpacesThinClientFullAccess 1513
Diese Richtlinie wird verwendet 1513
Einzelheiten zur Richtlinie 1514
Version der Richtlinie 1514
JSON-Richtliniendokument 1514
Weitere Informationen 1515
AmazonWorkSpacesThinClientMonitoringServiceRolePolicy 1516
Diese Richtlinie wird verwendet 1516
Einzelheiten der Richtlinie 1516
Version der Richtlinie 1516
JSON-Richtliniendokument 1516
Weitere Informationen 1517
AmazonWorkSpacesThinClientReadOnlyAccess 1517
Diese Richtlinie wird verwendet 1517
Einzelheiten zur Richtlinie 1517
Version der Richtlinie 1518
JSON-Richtliniendokument 1518
Weitere Informationen 1519
AmazonWorkSpacesWebReadOnly 1519
Diese Richtlinie wird verwendet 1519
Einzelheiten zur Richtlinie 1520
Version der Richtlinie 1520
JSON-Richtliniendokument 1520
Weitere Informationen 1521
AmazonWorkSpacesWebServiceRolePolicy 1521
Diese Richtlinie wird verwendet 1521
Einzelheiten der Richtlinie 1522
Version der Richtlinie 1522
JSON-Richtliniendokument 1522
Weitere Informationen 1524
AmazonZocaloFullAccess 1524
Diese Richtlinie wird verwendet 1525
Einzelheiten zur Richtlinie 1525
Version der Richtlinie 1525
JSON-Richtliniendokument 1525
Weitere Informationen 1526

AmazonZocaloReadOnlyAccess 1526
Diese Richtlinie wird verwendet 1526
Einzelheiten zur Richtlinie 1526
Version der Richtlinie 1527
JSON-Richtliniendokument 1527
Weitere Informationen 1527
AmplifyBackendDeployFullAccess 1528
Diese Richtlinie wird verwendet 1528
Einzelheiten zur Richtlinie 1528
Version der Richtlinie 1528
JSON-Richtliniendokument 1528
Weitere Informationen 1533
APIGatewayServiceRolePolicy 1533
Diese Richtlinie wird verwendet 1533
Einzelheiten der Richtlinie 1533
Version der Richtlinie 1533
JSON-Richtliniendokument 1534
Weitere Informationen 1536
AppIntegrationsServiceLinkedRolePolicy 1536
Diese Richtlinie wird verwendet 1536
Einzelheiten der Richtlinie 1536
Version der Richtlinie 1537
JSON-Richtliniendokument 1537
Weitere Informationen 1538
ApplicationAutoScalingForAmazonAppStreamAccess 1539
Diese Richtlinie wird verwendet 1539
Einzelheiten zur Richtlinie 1539
Version der Richtlinie 1539
JSON-Richtliniendokument 1539
Weitere Informationen 1540
ApplicationDiscoveryServiceContinuousExportServiceRolePolicy 1540
Diese Richtlinie wird verwendet 1540
Einzelheiten der Richtlinie 1541
Version der Richtlinie 1541
JSON-Richtliniendokument 1541
Weitere Informationen 1543

AppRunnerNetworkingServiceRolePolicy 1543
Diese Richtlinie wird verwendet 1543
Einzelheiten der Richtlinie 1543
Version der Richtlinie 1544
JSON-Richtliniendokument 1544
Weitere Informationen 1545
AppRunnerServiceRolePolicy 1545
Diese Richtlinie wird verwendet 1546
Einzelheiten der Richtlinie 1546
Version der Richtlinie 1546
JSON-Richtliniendokument 1546
Weitere Informationen 1547
AppStudioServiceRolePolicy 1547
Diese Richtlinie wird verwendet 1547
Einzelheiten der Richtlinie 1548
Version der Richtlinie 1548
JSON-Richtliniendokument 1548
Weitere Informationen 1550
AuroraDsqlServiceLinkedRolePolicy 1550
Diese Richtlinie wird verwendet 1551
Einzelheiten der Richtlinie 1551
Version der Richtlinie 1551
JSON-Richtliniendokument 1551
Weitere Informationen 1552
AutoScalingConsoleFullAccess 1552
Diese Richtlinie wird verwendet 1552
Einzelheiten zur Richtlinie 1552
Version der Richtlinie 1552
JSON-Richtliniendokument 1553
Weitere Informationen 1554
AutoScalingConsoleReadOnlyAccess 1555
Diese Richtlinie wird verwendet 1555
Einzelheiten zur Richtlinie 1555
Version der Richtlinie 1555
JSON-Richtliniendokument 1555
Weitere Informationen 1556

AutoScalingFullAccess 1557
Diese Richtlinie wird verwendet 1557
Einzelheiten zur Richtlinie 1557
Version der Richtlinie 1557
JSON-Richtliniendokument 1557
Weitere Informationen 1558
AutoScalingNotificationAccessRole 1559
Diese Richtlinie wird verwendet 1559
Einzelheiten zur Richtlinie 1559
Version der Richtlinie 1559
JSON-Richtliniendokument 1559
Weitere Informationen 1560
AutoScalingReadOnlyAccess 1560
Diese Richtlinie wird verwendet 1560
Einzelheiten zur Richtlinie 1560
Version der Richtlinie 1561
JSON-Richtliniendokument 1561
Weitere Informationen 1561
AutoScalingServiceRolePolicy 1561
Diese Richtlinie wird verwendet 1562
Einzelheiten der Richtlinie 1562
Version der Richtlinie 1562
JSON-Richtliniendokument 1562
Weitere Informationen 1565
AWS-SSM-Automation-DiagnosisBucketPolicy 1565
Diese Richtlinie wird verwendet 1566
Einzelheiten zur Richtlinie 1566
Version der Richtlinie 1566
JSON-Richtliniendokument 1566
Weitere Informationen 1568
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy 1569
Diese Richtlinie wird verwendet 1569
Einzelheiten zur Richtlinie 1569
Version der Richtlinie 1569
JSON-Richtliniendokument 1569
Weitere Informationen 1572

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy 1572
Diese Richtlinie wird verwendet 1572
Einzelheiten zur Richtlinie 1572
Version der Richtlinie 1573
JSON-Richtliniendokument 1573
Weitere Informationen 1575
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy 1575
Diese Richtlinie wird verwendet 1575
Einzelheiten zur Richtlinie 1575
Version der Richtlinie 1576
JSON-Richtliniendokument 1576
Weitere Informationen 1577
AWS-SSM-RemediationAutomation-AdministrationRolePolicy 1577
Diese Richtlinie wird verwendet 1577
Einzelheiten zur Richtlinie 1577
Version der Richtlinie 1578
JSON-Richtliniendokument 1578
Weitere Informationen 1580
AWS-SSM-RemediationAutomation-ExecutionRolePolicy 1580
Diese Richtlinie wird verwendet 1581
Einzelheiten zur Richtlinie 1581
Version der Richtlinie 1581
JSON-Richtliniendokument 1581
Weitere Informationen 1587
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy 1588
Diese Richtlinie wird verwendet 1588
Einzelheiten zur Richtlinie 1588
Version der Richtlinie 1588
JSON-Richtliniendokument 1589
Weitere Informationen 1589
AWS_ConfigRole 1590
Diese Richtlinie wird verwendet 1590
Einzelheiten zur Richtlinie 1590
Version der Richtlinie 1590
JSON-Richtliniendokument 1590
Weitere Informationen 1633

AWSAccountActivityAccess 1634
Diese Richtlinie wird verwendet 1634
Einzelheiten zur Richtlinie 1634
Version der Richtlinie 1634
JSON-Richtliniendokument 1634
Weitere Informationen 1635
AWSAccountManagementFullAccess 1635
Diese Richtlinie wird verwendet 1635
Einzelheiten zur Richtlinie 1635
Version der Richtlinie 1636
JSON-Richtliniendokument 1636
Weitere Informationen 1636
AWSAccountManagementReadOnlyAccess 1636
Diese Richtlinie wird verwendet 1637
Einzelheiten zur Richtlinie 1637
Version der Richtlinie 1637
JSON-Richtliniendokument 1637
Weitere Informationen 1638
AWSAccountSettingsManagementRole 1638
Diese Richtlinie wird verwendet 1638
Einzelheiten zur Richtlinie 1638
Version der Richtlinie 1638
JSON-Richtliniendokument 1639
Weitere Informationen 1641
AWSAccountUsageReportAccess 1641
Diese Richtlinie wird verwendet 1641
Einzelheiten zur Richtlinie 1641
Version der Richtlinie 1642
JSON-Richtliniendokument 1642
Weitere Informationen 1642
AWSAgentlessDiscoveryService 1642
Diese Richtlinie wird verwendet 1643
Einzelheiten zur Richtlinie 1643
Version der Richtlinie 1643
JSON-Richtliniendokument 1643
Weitere Informationen 1645

AWSAppFabricFullAccess 1645
Diese Richtlinie wird verwendet 1645
Einzelheiten zur Richtlinie 1645
Version der Richtlinie 1646
JSON-Richtliniendokument 1646
Weitere Informationen 1647
AWSAppFabricReadOnlyAccess 1647
Diese Richtlinie wird verwendet 1647
Einzelheiten zur Richtlinie 1648
Version der Richtlinie 1648
JSON-Richtliniendokument 1648
Weitere Informationen 1649
AWSAppFabricServiceRolePolicy 1649
Diese Richtlinie wird verwendet 1649
Einzelheiten der Richtlinie 1649
Version der Richtlinie 1649
JSON-Richtliniendokument 1650
Weitere Informationen 1651
AWSApplicationAutoscalingAppStreamFleetPolicy 1651
Diese Richtlinie wird verwendet 1651
Einzelheiten der Richtlinie 1651
Version der Richtlinie 1651
JSON-Richtliniendokument 1652
Weitere Informationen 1652
AWSApplicationAutoscalingCassandraTablePolicy 1652
Diese Richtlinie wird verwendet 1653
Einzelheiten der Richtlinie 1653
Version der Richtlinie 1653
JSON-Richtliniendokument 1653
Weitere Informationen 1654
AWSApplicationAutoscalingComprehendEndpointPolicy 1654
Diese Richtlinie wird verwendet 1654
Einzelheiten der Richtlinie 1654
Version der Richtlinie 1655
JSON-Richtliniendokument 1655
Weitere Informationen 1655

AWSApplicationAutoScalingCustomResourcePolicy 1655
Diese Richtlinie wird verwendet 1656
Einzelheiten der Richtlinie 1656
Version der Richtlinie 1656
JSON-Richtliniendokument 1656
Weitere Informationen 1657
AWSApplicationAutoscalingDynamoDBTablePolicy 1657
Diese Richtlinie wird verwendet 1657
Einzelheiten der Richtlinie 1657
Version der Richtlinie 1657
JSON-Richtliniendokument 1658
Weitere Informationen 1658
AWSApplicationAutoscalingEC2SpotFleetRequestPolicy 1658
Diese Richtlinie wird verwendet 1659
Einzelheiten der Richtlinie 1659
Version der Richtlinie 1659
JSON-Richtliniendokument 1659
Weitere Informationen 1660
AWSApplicationAutoscalingECSServicePolicy 1660
Diese Richtlinie wird verwendet 1660
Einzelheiten der Richtlinie 1660
Version der Richtlinie 1660
JSON-Richtliniendokument 1661
Weitere Informationen 1661
AWSApplicationAutoscalingElastiCacheRGPolicy 1661
Diese Richtlinie wird verwendet 1662
Einzelheiten der Richtlinie 1662
Version der Richtlinie 1662
JSON-Richtliniendokument 1662
Weitere Informationen 1663
AWSApplicationAutoscalingEMRInstanceGroupPolicy 1663
Diese Richtlinie wird verwendet 1664
Einzelheiten der Richtlinie 1664
Version der Richtlinie 1664
JSON-Richtliniendokument 1664
Weitere Informationen 1665

AWSApplicationAutoscalingKafkaClusterPolicy 1665
Diese Richtlinie wird verwendet 1665
Einzelheiten der Richtlinie 1665
Version der Richtlinie 1665
JSON-Richtliniendokument 1666
Weitere Informationen 1666
AWSApplicationAutoscalingLambdaConcurrencyPolicy 1666
Diese Richtlinie wird verwendet 1667
Einzelheiten der Richtlinie 1667
Version der Richtlinie 1667
JSON-Richtliniendokument 1667
Weitere Informationen 1668
AWSApplicationAutoscalingNeptuneClusterPolicy 1668
Diese Richtlinie wird verwendet 1668
Einzelheiten der Richtlinie 1668
Version der Richtlinie 1668
JSON-Richtliniendokument 1669
Weitere Informationen 1670
AWSApplicationAutoscalingRDSClusterPolicy 1670
Diese Richtlinie wird verwendet 1671
Einzelheiten der Richtlinie 1671
Version der Richtlinie 1671
JSON-Richtliniendokument 1671
Weitere Informationen 1672
AWSApplicationAutoscalingSageMakerEndpointPolicy 1672
Diese Richtlinie wird verwendet 1672
Einzelheiten der Richtlinie 1673
Version der Richtlinie 1673
JSON-Richtliniendokument 1673
Weitere Informationen 1674
AWSApplicationAutoscalingWorkSpacesPoolPolicy 1674
Diese Richtlinie wird verwendet 1674
Einzelheiten der Richtlinie 1674
Version der Richtlinie 1675
JSON-Richtliniendokument 1675
Weitere Informationen 1676

AWSApplicationDiscoveryAgentAccess 1676
Diese Richtlinie wird verwendet 1676
Einzelheiten zur Richtlinie 1677
Version der Richtlinie 1677
JSON-Richtliniendokument 1677
Weitere Informationen 1678
AWSApplicationDiscoveryAgentlessCollectorAccess 1678
Diese Richtlinie wird verwendet 1678
Einzelheiten zur Richtlinie 1678
Version der Richtlinie 1678
JSON-Richtliniendokument 1679
Weitere Informationen 1680
AWSApplicationDiscoveryServiceFullAccess 1680
Diese Richtlinie wird verwendet 1680
Einzelheiten zur Richtlinie 1680
Version der Richtlinie 1680
JSON-Richtliniendokument 1681
Weitere Informationen 1682
AWSApplicationMigrationAgentInstallationPolicy 1682
Diese Richtlinie wird verwendet 1682
Einzelheiten zur Richtlinie 1683
Version der Richtlinie 1683
JSON-Richtliniendokument 1683
Weitere Informationen 1684
AWSApplicationMigrationAgentPolicy 1684
Diese Richtlinie wird verwendet 1684
Einzelheiten zur Richtlinie 1684
Version der Richtlinie 1685
JSON-Richtliniendokument 1685
Weitere Informationen 1686
AWSApplicationMigrationAgentPolicy_v2 1686
Diese Richtlinie wird verwendet 1686
Einzelheiten zur Richtlinie 1686
Version der Richtlinie 1687
JSON-Richtliniendokument 1687
Weitere Informationen 1687

AWSApplicationMigrationConversionServerPolicy 1688
Diese Richtlinie wird verwendet 1688
Einzelheiten zur Richtlinie 1688
Version der Richtlinie 1688
JSON-Richtliniendokument 1689
Weitere Informationen 1689
AWSApplicationMigrationEC2Access 1689
Diese Richtlinie wird verwendet 1690
Einzelheiten zur Richtlinie 1690
Version der Richtlinie 1690
JSON-Richtliniendokument 1690
Weitere Informationen 1698
AWSApplicationMigrationFullAccess 1698
Diese Richtlinie wird verwendet 1699
Einzelheiten zur Richtlinie 1699
Version der Richtlinie 1699
JSON-Richtliniendokument 1699
Weitere Informationen 1705
AWSApplicationMigrationMGHAccess 1705
Diese Richtlinie wird verwendet 1706
Einzelheiten zur Richtlinie 1706
Version der Richtlinie 1706
JSON-Richtliniendokument 1706
Weitere Informationen 1707
AWSApplicationMigrationNetworkMigrationCustomResource 1707
Diese Richtlinie wird verwendet 1707
Einzelheiten zur Richtlinie 1707
Version der Richtlinie 1707
JSON-Richtliniendokument 1708
Weitere Informationen 1708
AWSApplicationMigrationNetworkMigrationMultiAccount 1709
Diese Richtlinie wird verwendet 1709
Einzelheiten zur Richtlinie 1709
Version der Richtlinie 1709
JSON-Richtliniendokument 1709
Weitere Informationen 1734

AWSApplicationMigrationReadOnlyAccess 1734
Diese Richtlinie wird verwendet 1734
Einzelheiten zur Richtlinie 1734
Version der Richtlinie 1734
JSON-Richtliniendokument 1735
Weitere Informationen 1736
AWSApplicationMigrationReplicationServerPolicy 1736
Diese Richtlinie wird verwendet 1736
Einzelheiten zur Richtlinie 1736
Version der Richtlinie 1737
JSON-Richtliniendokument 1737
Weitere Informationen 1738
AWSApplicationMigrationServiceEc2InstancePolicy 1739
Diese Richtlinie wird verwendet 1739
Einzelheiten zur Richtlinie 1739
Version der Richtlinie 1739
JSON-Richtliniendokument 1740
Weitere Informationen 1741
AWSApplicationMigrationServiceRolePolicy 1741
Diese Richtlinie wird verwendet 1741
Einzelheiten der Richtlinie 1741
Version der Richtlinie 1741
JSON-Richtliniendokument 1742
Weitere Informationen 1749
AWSApplicationMigrationSSMAccess 1749
Diese Richtlinie wird verwendet 1749
Einzelheiten zur Richtlinie 1750
Version der Richtlinie 1750
JSON-Richtliniendokument 1750
Weitere Informationen 1752
AWSApplicationMigrationVCenterClientPolicy 1752
Diese Richtlinie wird verwendet 1752
Einzelheiten zur Richtlinie 1752
Version der Richtlinie 1753
JSON-Richtliniendokument 1753
Weitere Informationen 1754

AWSAppMeshEnvoyAccess 1754
Diese Richtlinie wird verwendet 1754
Einzelheiten zur Richtlinie 1754
Version der Richtlinie 1754
JSON-Richtliniendokument 1754
Weitere Informationen 1755
AWSAppMeshFullAccess 1755
Diese Richtlinie wird verwendet 1755
Einzelheiten zur Richtlinie 1755
Version der Richtlinie 1756
JSON-Richtliniendokument 1756
Weitere Informationen 1757
AWSAppMeshPreviewEnvoyAccess 1757
Diese Richtlinie wird verwendet 1758
Einzelheiten zur Richtlinie 1758
Version der Richtlinie 1758
JSON-Richtliniendokument 1758
Weitere Informationen 1758
AWSAppMeshPreviewServiceRolePolicy 1759
Diese Richtlinie wird verwendet 1759
Einzelheiten der Richtlinie 1759
Version der Richtlinie 1759
JSON-Richtliniendokument 1759
Weitere Informationen 1760
AWSAppMeshReadOnly 1760
Diese Richtlinie wird verwendet 1760
Einzelheiten zur Richtlinie 1760
Version der Richtlinie 1761
JSON-Richtliniendokument 1761
Weitere Informationen 1762
AWSAppMeshServiceRolePolicy 1762
Diese Richtlinie wird verwendet 1762
Einzelheiten der Richtlinie 1762
Version der Richtlinie 1763
JSON-Richtliniendokument 1763
Weitere Informationen 1763

AWSAppRunnerFullAccess 1764
Diese Richtlinie wird verwendet 1764
Einzelheiten zur Richtlinie 1764
Version der Richtlinie 1764
JSON-Richtliniendokument 1764
Weitere Informationen 1765
AWSAppRunnerReadOnlyAccess 1765
Diese Richtlinie wird verwendet 1766
Einzelheiten zur Richtlinie 1766
Version der Richtlinie 1766
JSON-Richtliniendokument 1766
Weitere Informationen 1766
AWSAppRunnerServicePolicyForECRAccess 1767
Diese Richtlinie wird verwendet 1767
Einzelheiten zur Richtlinie 1767
Version der Richtlinie 1767
JSON-Richtliniendokument 1768
Weitere Informationen 1768
AWSAppSyncAdministrator 1768
Diese Richtlinie wird verwendet 1768
Einzelheiten zur Richtlinie 1769
Version der Richtlinie 1769
JSON-Richtliniendokument 1769
Weitere Informationen 1770
AWSAppSyncInvokeFullAccess 1770
Diese Richtlinie wird verwendet 1771
Einzelheiten zur Richtlinie 1771
Version der Richtlinie 1771
JSON-Richtliniendokument 1771
Weitere Informationen 1772
AWSAppSyncPushToCloudWatchLogs 1772
Diese Richtlinie wird verwendet 1772
Einzelheiten zur Richtlinie 1772
Version der Richtlinie 1772
JSON-Richtliniendokument 1772
Weitere Informationen 1773

AWSAppSyncSchemaAuthor 1773
Diese Richtlinie wird verwendet 1773
Einzelheiten zur Richtlinie 1773
Version der Richtlinie 1774
JSON-Richtliniendokument 1774
Weitere Informationen 1775
AWSAppSyncServiceRolePolicy 1775
Diese Richtlinie wird verwendet 1775
Einzelheiten der Richtlinie 1775
Version der Richtlinie 1776
JSON-Richtliniendokument 1776
Weitere Informationen 1776
AWSArtifactAccountSync 1776
Diese Richtlinie wird verwendet 1777
Einzelheiten zur Richtlinie 1777
Version der Richtlinie 1777
JSON-Richtliniendokument 1777
Weitere Informationen 1778
AWSArtifactAgreementsFullAccess 1778
Diese Richtlinie wird verwendet 1778
Einzelheiten zur Richtlinie 1778
Version der Richtlinie 1778
JSON-Richtliniendokument 1779
Weitere Informationen 1781
AWSArtifactAgreementsReadOnlyAccess 1781
Diese Richtlinie wird verwendet 1781
Einzelheiten zur Richtlinie 1781
Version der Richtlinie 1781
JSON-Richtliniendokument 1782
Weitere Informationen 1783
AWSArtifactReportsReadOnlyAccess 1783
Diese Richtlinie wird verwendet 1783
Einzelheiten zur Richtlinie 1783
Version der Richtlinie 1783
JSON-Richtliniendokument 1784
Weitere Informationen 1784

AWSArtifactServiceRolePolicy 1784
Diese Richtlinie wird verwendet 1785
Einzelheiten der Richtlinie 1785
Version der Richtlinie 1785
JSON-Richtliniendokument 1785
Weitere Informationen 1786
AWSAuditManagerAdministratorAccess 1786
Diese Richtlinie wird verwendet 1786
Einzelheiten zur Richtlinie 1786
Version der Richtlinie 1786
JSON-Richtliniendokument 1787
Weitere Informationen 1791
AWSAuditManagerServiceRolePolicy 1791
Diese Richtlinie wird verwendet 1791
Einzelheiten der Richtlinie 1791
Version der Richtlinie 1791
JSON-Richtliniendokument 1792
Weitere Informationen 1798
AWSAutoScalingPlansEC2AutoScalingPolicy 1799
Diese Richtlinie wird verwendet 1799
Einzelheiten der Richtlinie 1799
Version der Richtlinie 1799
JSON-Richtliniendokument 1799
Weitere Informationen 1800
AWSBackupAuditAccess 1800
Diese Richtlinie wird verwendet 1800
Einzelheiten zur Richtlinie 1800
Version der Richtlinie 1801
JSON-Richtliniendokument 1801
Weitere Informationen 1802
AWSBackupDataTransferAccess 1802
Diese Richtlinie wird verwendet 1803
Einzelheiten zur Richtlinie 1803
Version der Richtlinie 1803
JSON-Richtliniendokument 1803
Weitere Informationen 1804

AWSBackupFullAccess 1804
Diese Richtlinie wird verwendet 1804
Einzelheiten zur Richtlinie 1804
Version der Richtlinie 1804
JSON-Richtliniendokument 1805
Weitere Informationen 1816
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 1817
Diese Richtlinie wird verwendet 1817
Einzelheiten zur Richtlinie 1817
Version der Richtlinie 1817
JSON-Richtliniendokument 1817
Weitere Informationen 1818
AWSBackupGuardDutyRolePolicyForScans 1818
Diese Richtlinie wird verwendet 1818
Einzelheiten zur Richtlinie 1818
Version der Richtlinie 1819
JSON-Richtliniendokument 1819
Weitere Informationen 1823
AWSBackupOperatorAccess 1823
Diese Richtlinie wird verwendet 1823
Einzelheiten zur Richtlinie 1823
Version der Richtlinie 1824
JSON-Richtliniendokument 1824
Weitere Informationen 1833
AWSBackupOrganizationAdminAccess 1833
Diese Richtlinie wird verwendet 1833
Einzelheiten zur Richtlinie 1833
Version der Richtlinie 1834
JSON-Richtliniendokument 1834
Weitere Informationen 1836
AWSBackupRestoreAccessForSAPHANA 1836
Diese Richtlinie wird verwendet 1836
Einzelheiten zur Richtlinie 1836
Version der Richtlinie 1836
JSON-Richtliniendokument 1837
Weitere Informationen 1837

AWSBackupSearchOperatorAccess 1838
Diese Richtlinie wird verwendet 1838
Einzelheiten zur Richtlinie 1838
Version der Richtlinie 1838
JSON-Richtliniendokument 1838
Weitere Informationen 1840
AWSBackupServiceLinkedRolePolicyForBackup 1840
Diese Richtlinie wird verwendet 1840
Einzelheiten der Richtlinie 1841
Version der Richtlinie 1841
JSON-Richtliniendokument 1841
Weitere Informationen 1851
AWSBackupServiceLinkedRolePolicyForBackupTest 1851
Diese Richtlinie wird verwendet 1852
Einzelheiten der Richtlinie 1852
Version der Richtlinie 1852
JSON-Richtliniendokument 1852
Weitere Informationen 1853
AWSBackupServiceRolePolicyForBackup 1853
Diese Richtlinie wird verwendet 1853
Einzelheiten zur Richtlinie 1853
Version der Richtlinie 1854
JSON-Richtliniendokument 1854
Weitere Informationen 1868
AWSBackupServiceRolePolicyForIndexing 1868
Diese Richtlinie wird verwendet 1868
Einzelheiten zur Richtlinie 1868
Version der Richtlinie 1869
JSON-Richtliniendokument 1869
Weitere Informationen 1870
AWSBackupServiceRolePolicyForItemRestores 1870
Diese Richtlinie wird verwendet 1870
Einzelheiten zur Richtlinie 1871
Version der Richtlinie 1871
JSON-Richtliniendokument 1871
Weitere Informationen 1873

AWSBackupServiceRolePolicyForRestores 1873
Diese Richtlinie wird verwendet 1873
Einzelheiten zur Richtlinie 1873
Version der Richtlinie 1874
JSON-Richtliniendokument 1874
Weitere Informationen 1888
AWSBackupServiceRolePolicyForS3Backup 1888
Diese Richtlinie wird verwendet 1888
Einzelheiten zur Richtlinie 1888
Version der Richtlinie 1888
JSON-Richtliniendokument 1889
Weitere Informationen 1891
AWSBackupServiceRolePolicyForS3Restore 1891
Diese Richtlinie wird verwendet 1891
Einzelheiten zur Richtlinie 1891
Version der Richtlinie 1892
JSON-Richtliniendokument 1892
Weitere Informationen 1893
AWSBackupServiceRolePolicyForScans 1893
Diese Richtlinie wird verwendet 1894
Einzelheiten zur Richtlinie 1894
Version der Richtlinie 1894
JSON-Richtliniendokument 1894
Weitere Informationen 1895
AWSBatchFullAccess 1895
Diese Richtlinie wird verwendet 1895
Einzelheiten zur Richtlinie 1895
Version der Richtlinie 1896
JSON-Richtliniendokument 1896
Weitere Informationen 1897
AWSBatchServiceEventTargetRole 1898
Diese Richtlinie wird verwendet 1898
Einzelheiten zur Richtlinie 1898
Version der Richtlinie 1898
JSON-Richtliniendokument 1898
Weitere Informationen 1899

AWSBatchServiceRole 1899
Diese Richtlinie wird verwendet 1899
Einzelheiten zur Richtlinie 1899
Version der Richtlinie 1899
JSON-Richtliniendokument 1900
Weitere Informationen 1903
AWSBatchServiceRolePolicyForSageMaker 1903
Diese Richtlinie wird verwendet 1903
Einzelheiten der Richtlinie 1903
Version der Richtlinie 1904
JSON-Richtliniendokument 1904
Weitere Informationen 1905
AWSBCMDataExportsServiceRolePolicy 1905
Diese Richtlinie wird verwendet 1906
Einzelheiten der Richtlinie 1906
Version der Richtlinie 1906
JSON-Richtliniendokument 1906
Weitere Informationen 1907
AWSBillingConductorFullAccess 1907
Diese Richtlinie wird verwendet 1907
Einzelheiten zur Richtlinie 1907
Version der Richtlinie 1907
JSON-Richtliniendokument 1907
Weitere Informationen 1908
AWSBillingConductorReadOnlyAccess 1908
Diese Richtlinie wird verwendet 1909
Einzelheiten zur Richtlinie 1909
Version der Richtlinie 1909
JSON-Richtliniendokument 1909
Weitere Informationen 1910
AWSBillingReadOnlyAccess 1910
Diese Richtlinie wird verwendet 1910
Einzelheiten zur Richtlinie 1910
Version der Richtlinie 1910
JSON-Richtliniendokument 1911
Weitere Informationen 1913

AWSBillingServiceRolePolicy 1913
Diese Richtlinie wird verwendet 1913
Einzelheiten der Richtlinie 1913
Version der Richtlinie 1913
JSON-Richtliniendokument 1914
Weitere Informationen 1914
AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM 1914
Diese Richtlinie wird verwendet 1914
Einzelheiten zur Richtlinie 1915
Version der Richtlinie 1915
JSON-Richtliniendokument 1915
Weitere Informationen 1916
AWSBudgetsActionsWithAWSResourceControlAccess 1916
Diese Richtlinie wird verwendet 1916
Einzelheiten zur Richtlinie 1916
Version der Richtlinie 1917
JSON-Richtliniendokument 1917
Weitere Informationen 1918
AWSBudgetsReadOnlyAccess 1918
Diese Richtlinie wird verwendet 1919
Einzelheiten zur Richtlinie 1919
Version der Richtlinie 1919
JSON-Richtliniendokument 1919
Weitere Informationen 1920
AWSBugBustFullAccess 1920
Diese Richtlinie wird verwendet 1920
Einzelheiten zur Richtlinie 1920
Version der Richtlinie 1920
JSON-Richtliniendokument 1920
Weitere Informationen 1922
AWSBugBustPlayerAccess 1922
Diese Richtlinie wird verwendet 1922
Einzelheiten zur Richtlinie 1922
Version der Richtlinie 1922
JSON-Richtliniendokument 1923
Weitere Informationen 1924

AWSBugBustServiceRolePolicy 1924
Diese Richtlinie wird verwendet 1924
Einzelheiten der Richtlinie 1924
Version der Richtlinie 1924
JSON-Richtliniendokument 1925
Weitere Informationen 1925
AWSCertificateManagerFullAccess 1925
Diese Richtlinie wird verwendet 1925
Einzelheiten zur Richtlinie 1926
Version der Richtlinie 1926
JSON-Richtliniendokument 1926
Weitere Informationen 1927
AWSCertificateManagerPrivateCAAuditor 1927
Diese Richtlinie wird verwendet 1927
Einzelheiten zur Richtlinie 1927
Version der Richtlinie 1928
JSON-Richtliniendokument 1928
Weitere Informationen 1928
AWSCertificateManagerPrivateCAFullAccess 1929
Diese Richtlinie wird verwendet 1929
Einzelheiten zur Richtlinie 1929
Version der Richtlinie 1929
JSON-Richtliniendokument 1929
Weitere Informationen 1930
AWSCertificateManagerPrivateCAPrivilegedUser 1930
Diese Richtlinie wird verwendet 1930
Einzelheiten zur Richtlinie 1930
Version der Richtlinie 1931
JSON-Richtliniendokument 1931
Weitere Informationen 1932
AWSCertificateManagerPrivateCAReadOnly 1932
Diese Richtlinie wird verwendet 1932
Einzelheiten zur Richtlinie 1933
Version der Richtlinie 1933
JSON-Richtliniendokument 1933
Weitere Informationen 1934

AWSCertificateManagerPrivateCAUser 1934
Diese Richtlinie wird verwendet 1934
Einzelheiten zur Richtlinie 1934
Version der Richtlinie 1934
JSON-Richtliniendokument 1935
Weitere Informationen 1936
AWSCertificateManagerReadOnly 1936
Diese Richtlinie wird verwendet 1936
Einzelheiten zur Richtlinie 1936
Version der Richtlinie 1936
JSON-Richtliniendokument 1937
Weitere Informationen 1937
AWSChatbotServiceLinkedRolePolicy 1937
Diese Richtlinie wird verwendet 1938
Einzelheiten der Richtlinie 1938
Version der Richtlinie 1938
JSON-Richtliniendokument 1938
Weitere Informationen 1939
AWSCleanRoomsFullAccess 1939
Diese Richtlinie wird verwendet 1939
Einzelheiten zur Richtlinie 1939
Version der Richtlinie 1940
JSON-Richtliniendokument 1940
Weitere Informationen 1944
AWSCleanRoomsFullAccessNoQuerying 1944
Diese Richtlinie wird verwendet 1945
Einzelheiten zur Richtlinie 1945
Version der Richtlinie 1945
JSON-Richtliniendokument 1945
Weitere Informationen 1950
AWSCleanRoomsMLFullAccess 1950
Diese Richtlinie wird verwendet 1950
Einzelheiten zur Richtlinie 1950
Version der Richtlinie 1951
JSON-Richtliniendokument 1951
Weitere Informationen 1955

AWSCleanRoomsMLReadOnlyAccess 1955
Diese Richtlinie wird verwendet 1955
Einzelheiten zur Richtlinie 1955
Version der Richtlinie 1955
JSON-Richtliniendokument 1956
Weitere Informationen 1957
AWSCleanRoomsReadOnlyAccess 1957
Diese Richtlinie wird verwendet 1957
Einzelheiten zur Richtlinie 1957
Version der Richtlinie 1958
JSON-Richtliniendokument 1958
Weitere Informationen 1959
AWSCleanRoomsServiceRolePolicy 1959
Diese Richtlinie wird verwendet 1959
Einzelheiten der Richtlinie 1959
Version der Richtlinie 1960
JSON-Richtliniendokument 1960
Weitere Informationen 1960
AWSCloud9Administrator 1961
Diese Richtlinie wird verwendet 1961
Einzelheiten zur Richtlinie 1961
Version der Richtlinie 1961
JSON-Richtliniendokument 1961
Weitere Informationen 1963
AWSCloud9EnvironmentMember 1963
Diese Richtlinie wird verwendet 1963
Einzelheiten zur Richtlinie 1963
Version der Richtlinie 1964
JSON-Richtliniendokument 1964
Weitere Informationen 1965
AWSCloud9ServiceRolePolicy 1966
Diese Richtlinie wird verwendet 1966
Einzelheiten der Richtlinie 1966
Version der Richtlinie 1966
JSON-Richtliniendokument 1966
Weitere Informationen 1969

AWSCloud9SSMInstanceProfile 1969
Diese Richtlinie wird verwendet 1969
Einzelheiten zur Richtlinie 1969
Version der Richtlinie 1969
JSON-Richtliniendokument 1970
Weitere Informationen 1970
AWSCloud9User 1970
Diese Richtlinie wird verwendet 1970
Einzelheiten zur Richtlinie 1971
Version der Richtlinie 1971
JSON-Richtliniendokument 1971
Weitere Informationen 1974
AWSCloudFormationFullAccess 1974
Diese Richtlinie wird verwendet 1974
Einzelheiten zur Richtlinie 1974
Version der Richtlinie 1974
JSON-Richtliniendokument 1974
Weitere Informationen 1975
AWSCloudFormationReadOnlyAccess 1975
Diese Richtlinie wird verwendet 1975
Einzelheiten zur Richtlinie 1975
Version der Richtlinie 1976
JSON-Richtliniendokument 1976
Weitere Informationen 1976
AWSCloudFrontLogger 1977
Diese Richtlinie wird verwendet 1977
Einzelheiten der Richtlinie 1977
Version der Richtlinie 1977
JSON-Richtliniendokument 1977
Weitere Informationen 1978
AWSCloudFrontVPCOriginServiceRolePolicy 1978
Diese Richtlinie wird verwendet 1978
Einzelheiten der Richtlinie 1978
Version der Richtlinie 1978
JSON-Richtliniendokument 1979
Weitere Informationen 1981

AWSCloudHSMFullAccess 1981
Diese Richtlinie wird verwendet 1982
Einzelheiten zur Richtlinie 1982
Version der Richtlinie 1982
JSON-Richtliniendokument 1982
Weitere Informationen 1982
AWSCloudHSMReadOnlyAccess 1983
Diese Richtlinie wird verwendet 1983
Einzelheiten zur Richtlinie 1983
Version der Richtlinie 1983
JSON-Richtliniendokument 1983
Weitere Informationen 1984
AWSCloudHSMRole 1984
Diese Richtlinie wird verwendet 1984
Einzelheiten zur Richtlinie 1984
Version der Richtlinie 1985
JSON-Richtliniendokument 1985
Weitere Informationen 1985
AWSCloudMapDiscoverInstanceAccess 1986
Diese Richtlinie wird verwendet 1986
Einzelheiten zur Richtlinie 1986
Version der Richtlinie 1986
JSON-Richtliniendokument 1986
Weitere Informationen 1987
AWSCloudMapFullAccess 1987
Diese Richtlinie wird verwendet 1987
Einzelheiten zur Richtlinie 1987
Version der Richtlinie 1987
JSON-Richtliniendokument 1988
Weitere Informationen 1988
AWSCloudMapReadOnlyAccess 1989
Diese Richtlinie wird verwendet 1989
Einzelheiten zur Richtlinie 1989
Version der Richtlinie 1989
JSON-Richtliniendokument 1989
Weitere Informationen 1990

AWSCloudMapRegisterInstanceAccess 1990
Diese Richtlinie wird verwendet 1990
Einzelheiten zur Richtlinie 1990
Version der Richtlinie 1990
JSON-Richtliniendokument 1991
Weitere Informationen 1991
AWSCloudShellFullAccess 1992
Diese Richtlinie wird verwendet 1992
Einzelheiten zur Richtlinie 1992
Version der Richtlinie 1992
JSON-Richtliniendokument 1992
Weitere Informationen 1993
AWSCloudTrail_FullAccess 1993
Diese Richtlinie wird verwendet 1993
Einzelheiten zur Richtlinie 1993
Version der Richtlinie 1993
JSON-Richtliniendokument 1994
Weitere Informationen 1996
AWSCloudTrail_ReadOnlyAccess 1996
Diese Richtlinie wird verwendet 1996
Einzelheiten zur Richtlinie 1997
Version der Richtlinie 1997
JSON-Richtliniendokument 1997
Weitere Informationen 1997
AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy 1998
Diese Richtlinie wird verwendet 1998
Einzelheiten der Richtlinie 1998
Version der Richtlinie 1998
JSON-Richtliniendokument 1999
Weitere Informationen 1999
AWSCodeArtifactAdminAccess 1999
Diese Richtlinie wird verwendet 1999
Einzelheiten zur Richtlinie 1999
Version der Richtlinie 2000
JSON-Richtliniendokument 2000
Weitere Informationen 2000

AWSCodeArtifactReadOnlyAccess 2001
Diese Richtlinie wird verwendet 2001
Einzelheiten zur Richtlinie 2001
Version der Richtlinie 2001
JSON-Richtliniendokument 2001
Weitere Informationen 2002
AWSCodeBuildAdminAccess 2002
Diese Richtlinie wird verwendet 2002
Einzelheiten zur Richtlinie 2003
Version der Richtlinie 2003
JSON-Richtliniendokument 2003
Weitere Informationen 2006
AWSCodeBuildDeveloperAccess 2007
Diese Richtlinie wird verwendet 2007
Einzelheiten zur Richtlinie 2007
Version der Richtlinie 2007
JSON-Richtliniendokument 2007
Weitere Informationen 2010
AWSCodeBuildReadOnlyAccess 2010
Diese Richtlinie wird verwendet 2010
Einzelheiten zur Richtlinie 2010
Version der Richtlinie 2011
JSON-Richtliniendokument 2011
Weitere Informationen 2012
AWSCodeCommitFullAccess 2013
Diese Richtlinie wird verwendet 2013
Einzelheiten zur Richtlinie 2013
Version der Richtlinie 2013
JSON-Richtliniendokument 2013
Weitere Informationen 2018
AWSCodeCommitPowerUser 2018
Diese Richtlinie wird verwendet 2018
Einzelheiten zur Richtlinie 2018
Version der Richtlinie 2018
JSON-Richtliniendokument 2019
Weitere Informationen 2023

AWSCodeCommitReadOnly 2024
Diese Richtlinie wird verwendet 2024
Einzelheiten zur Richtlinie 2024
Version der Richtlinie 2024
JSON-Richtliniendokument 2024
Weitere Informationen 2027
AWSCodeDeployDeployerAccess 2027
Diese Richtlinie wird verwendet 2027
Einzelheiten zur Richtlinie 2027
Version der Richtlinie 2028
JSON-Richtliniendokument 2028
Weitere Informationen 2029
AWSCodeDeployFullAccess 2030
Diese Richtlinie wird verwendet 2030
Einzelheiten zur Richtlinie 2030
Version der Richtlinie 2030
JSON-Richtliniendokument 2030
Weitere Informationen 2032
AWSCodeDeployReadOnlyAccess 2032
Diese Richtlinie wird verwendet 2032
Einzelheiten zur Richtlinie 2032
Version der Richtlinie 2032
JSON-Richtliniendokument 2033
Weitere Informationen 2034
AWSCodeDeployRole 2034
Diese Richtlinie wird verwendet 2034
Einzelheiten zur Richtlinie 2034
Version der Richtlinie 2034
JSON-Richtliniendokument 2035
Weitere Informationen 2036
AWSCodeDeployRoleForCloudFormation 2036
Diese Richtlinie wird verwendet 2036
Einzelheiten zur Richtlinie 2036
Version der Richtlinie 2037
JSON-Richtliniendokument 2037
Weitere Informationen 2037

AWSCodeDeployRoleForECS 2038
Diese Richtlinie wird verwendet 2038
Einzelheiten zur Richtlinie 2038
Version der Richtlinie 2038
JSON-Richtliniendokument 2038
Weitere Informationen 2039
AWSCodeDeployRoleForECSLimited 2040
Diese Richtlinie wird verwendet 2040
Einzelheiten zur Richtlinie 2040
Version der Richtlinie 2040
JSON-Richtliniendokument 2040
Weitere Informationen 2042
AWSCodeDeployRoleForLambda 2042
Diese Richtlinie wird verwendet 2042
Einzelheiten zur Richtlinie 2042
Version der Richtlinie 2043
JSON-Richtliniendokument 2043
Weitere Informationen 2044
AWSCodeDeployRoleForLambdaLimited 2044
Diese Richtlinie wird verwendet 2044
Einzelheiten zur Richtlinie 2045
Version der Richtlinie 2045
JSON-Richtliniendokument 2045
Weitere Informationen 2046
AWSCodePipeline_FullAccess 2046
Diese Richtlinie wird verwendet 2046
Einzelheiten zur Richtlinie 2047
Version der Richtlinie 2047
JSON-Richtliniendokument 2047
Weitere Informationen 2051
AWSCodePipeline_ReadOnlyAccess 2051
Diese Richtlinie wird verwendet 2051
Einzelheiten zur Richtlinie 2051
Version der Richtlinie 2051
JSON-Richtliniendokument 2052
Weitere Informationen 2053

AWSCodePipelineApproverAccess 2053
Diese Richtlinie wird verwendet 2053
Einzelheiten zur Richtlinie 2053
Version der Richtlinie 2053
JSON-Richtliniendokument 2054
Weitere Informationen 2054
AWSCodePipelineCustomActionAccess 2054
Diese Richtlinie wird verwendet 2055
Einzelheiten zur Richtlinie 2055
Version der Richtlinie 2055
JSON-Richtliniendokument 2055
Weitere Informationen 2056
AWSCodeStarFullAccess 2056
Diese Richtlinie wird verwendet 2056
Einzelheiten zur Richtlinie 2056
Version der Richtlinie 2056
JSON-Richtliniendokument 2057
Weitere Informationen 2057
AWSCodeStarNotificationsServiceRolePolicy 2058
Diese Richtlinie wird verwendet 2058
Einzelheiten der Richtlinie 2058
Version der Richtlinie 2058
JSON-Richtliniendokument 2058
Weitere Informationen 2060
AWSCodeStarServiceRole 2060
Diese Richtlinie wird verwendet 2060
Einzelheiten zur Richtlinie 2060
Version der Richtlinie 2060
JSON-Richtliniendokument 2060
Weitere Informationen 2065
AWSCompromisedKeyQuarantine 2065
Diese Richtlinie wird verwendet 2066
Einzelheiten zur Richtlinie 2066
Version der Richtlinie 2066
JSON-Richtliniendokument 2066
Weitere Informationen 2067

AWSCompromisedKeyQuarantineV2 2068
Diese Richtlinie wird verwendet 2068
Einzelheiten zur Richtlinie 2068
Version der Richtlinie 2068
JSON-Richtliniendokument 2068
Weitere Informationen 2071
AWSCompromisedKeyQuarantineV3 2071
Diese Richtlinie wird verwendet 2071
Einzelheiten zur Richtlinie 2071
Version der Richtlinie 2072
JSON-Richtliniendokument 2072
Weitere Informationen 2074
AWSConfigMultiAccountSetupPolicy 2074
Diese Richtlinie wird verwendet 2075
Einzelheiten der Richtlinie 2075
Version der Richtlinie 2075
JSON-Richtliniendokument 2075
Weitere Informationen 2077
AWSConfigRemediationServiceRolePolicy 2077
Diese Richtlinie wird verwendet 2077
Einzelheiten der Richtlinie 2078
Version der Richtlinie 2078
JSON-Richtliniendokument 2078
Weitere Informationen 2079
AWSConfigRoleForOrganizations 2079
Diese Richtlinie wird verwendet 2079
Einzelheiten zur Richtlinie 2079
Version der Richtlinie 2079
JSON-Richtliniendokument 2080
Weitere Informationen 2080
AWSConfigRulesExecutionRole 2080
Diese Richtlinie wird verwendet 2080
Einzelheiten zur Richtlinie 2081
Version der Richtlinie 2081
JSON-Richtliniendokument 2081
Weitere Informationen 2082

AWSConfigServiceRolePolicy 2082
Diese Richtlinie wird verwendet 2082
Einzelheiten der Richtlinie 2082
Version der Richtlinie 2082
JSON-Richtliniendokument 2083
Weitere Informationen 2127
AWSConfigUserAccess 2127
Diese Richtlinie wird verwendet 2127
Einzelheiten zur Richtlinie 2127
Version der Richtlinie 2127
JSON-Richtliniendokument 2127
Weitere Informationen 2128
AWSConnector 2128
Diese Richtlinie wird verwendet 2128
Einzelheiten zur Richtlinie 2129
Version der Richtlinie 2129
JSON-Richtliniendokument 2129
Weitere Informationen 2131
AWSControlTowerAccountServiceRolePolicy 2131
Diese Richtlinie wird verwendet 2131
Einzelheiten der Richtlinie 2131
Version der Richtlinie 2132
JSON-Richtliniendokument 2132
Weitere Informationen 2137
AWSControlTowerCloudTrailRolePolicy 2137
Diese Richtlinie wird verwendet 2137
Einzelheiten zur Richtlinie 2137
Version der Richtlinie 2138
JSON-Richtliniendokument 2138
Weitere Informationen 2138
AWSControlTowerIdentityCenterManagementPolicy 2139
Diese Richtlinie wird verwendet 2139
Einzelheiten zur Richtlinie 2139
Version der Richtlinie 2139
JSON-Richtliniendokument 2139
Weitere Informationen 2141

AWSControlTowerServiceRolePolicy 2141
Diese Richtlinie wird verwendet 2141
Einzelheiten zur Richtlinie 2141
Version der Richtlinie 2141
JSON-Richtliniendokument 2142
Weitere Informationen 2146
AWSCostAndUsageReportAutomationPolicy 2147
Diese Richtlinie wird verwendet 2147
Einzelheiten zur Richtlinie 2147
Version der Richtlinie 2147
JSON-Richtliniendokument 2147
Weitere Informationen 2148
AWSDataExchangeDataGrantOwnerFullAccess 2149
Diese Richtlinie wird verwendet 2149
Einzelheiten zur Richtlinie 2149
Version der Richtlinie 2149
JSON-Richtliniendokument 2149
Weitere Informationen 2151
AWSDataExchangeDataGrantReceiverFullAccess 2151
Diese Richtlinie wird verwendet 2151
Einzelheiten zur Richtlinie 2151
Version der Richtlinie 2152
JSON-Richtliniendokument 2152
Weitere Informationen 2153
AWSDataExchangeFullAccess 2154
Diese Richtlinie wird verwendet 2154
Einzelheiten zur Richtlinie 2154
Version der Richtlinie 2154
JSON-Richtliniendokument 2154
Weitere Informationen 2158
AWSDataExchangeProviderFullAccess 2158
Diese Richtlinie wird verwendet 2158
Einzelheiten zur Richtlinie 2158
Version der Richtlinie 2158
JSON-Richtliniendokument 2159
Weitere Informationen 2163

AWSDataExchangeReadOnly 2163
Diese Richtlinie wird verwendet 2163
Einzelheiten zur Richtlinie 2163
Version der Richtlinie 2163
JSON-Richtliniendokument 2164
Weitere Informationen 2165
AWSDataExchangeServiceRolePolicyForLicenseManagement 2165
Diese Richtlinie wird verwendet 2165
Einzelheiten der Richtlinie 2165
Version der Richtlinie 2166
JSON-Richtliniendokument 2166
Weitere Informationen 2166
AWSDataExchangeServiceRolePolicyForOrganizationDiscovery 2167
Diese Richtlinie wird verwendet 2167
Einzelheiten der Richtlinie 2167
Version der Richtlinie 2167
JSON-Richtliniendokument 2167
Weitere Informationen 2168
AWSDataExchangeSubscriberFullAccess 2168
Diese Richtlinie wird verwendet 2168
Einzelheiten zur Richtlinie 2168
Version der Richtlinie 2169
JSON-Richtliniendokument 2169
Weitere Informationen 2171
AWSDataLifecycleManagerServiceRole 2171
Diese Richtlinie wird verwendet 2171
Einzelheiten zur Richtlinie 2171
Version der Richtlinie 2172
JSON-Richtliniendokument 2172
Weitere Informationen 2173
AWSDataLifecycleManagerServiceRoleForAMIManagement 2173
Diese Richtlinie wird verwendet 2174
Einzelheiten zur Richtlinie 2174
Version der Richtlinie 2174
JSON-Richtliniendokument 2174
Weitere Informationen 2175

AWSDataLifecycleManagerSSMFullAccess 2176
Diese Richtlinie wird verwendet 2176
Einzelheiten zur Richtlinie 2176
Version der Richtlinie 2176
JSON-Richtliniendokument 2176
Weitere Informationen 2178
AWSDataPipeline_FullAccess 2178
Diese Richtlinie wird verwendet 2178
Einzelheiten zur Richtlinie 2178
Version der Richtlinie 2178
JSON-Richtliniendokument 2179
Weitere Informationen 2180
AWSDataPipeline_PowerUser 2180
Diese Richtlinie wird verwendet 2180
Einzelheiten zur Richtlinie 2180
Version der Richtlinie 2180
JSON-Richtliniendokument 2181
Weitere Informationen 2181
AWSDataSyncDiscoveryServiceRolePolicy 2182
Diese Richtlinie wird verwendet 2182
Einzelheiten der Richtlinie 2182
Version der Richtlinie 2182
JSON-Richtliniendokument 2182
Weitere Informationen 2183
AWSDataSyncFullAccess 2184
Diese Richtlinie wird verwendet 2184
Einzelheiten zur Richtlinie 2184
Version der Richtlinie 2184
JSON-Richtliniendokument 2184
Weitere Informationen 2187
AWSDataSyncReadOnlyAccess 2187
Diese Richtlinie wird verwendet 2187
Einzelheiten zur Richtlinie 2187
Version der Richtlinie 2187
JSON-Richtliniendokument 2188
Weitere Informationen 2188

AWSDataSyncServiceRolePolicy 2189
Diese Richtlinie wird verwendet 2189
Einzelheiten der Richtlinie 2189
Version der Richtlinie 2189
JSON-Richtliniendokument 2189
Weitere Informationen 2190
AWSDeadlineCloud-FleetWorker 2191
Diese Richtlinie wird verwendet 2191
Einzelheiten zur Richtlinie 2191
Version der Richtlinie 2191
JSON-Richtliniendokument 2191
Weitere Informationen 2192
AWSDeadlineCloud-UserAccessFarms 2192
Diese Richtlinie wird verwendet 2192
Einzelheiten zur Richtlinie 2192
Version der Richtlinie 2193
JSON-Richtliniendokument 2193
Weitere Informationen 2198
AWSDeadlineCloud-UserAccessFleets 2198
Diese Richtlinie wird verwendet 2199
Einzelheiten zur Richtlinie 2199
Version der Richtlinie 2199
JSON-Richtliniendokument 2199
Weitere Informationen 2203
AWSDeadlineCloud-UserAccessJobs 2203
Diese Richtlinie wird verwendet 2203
Einzelheiten zur Richtlinie 2203
Version der Richtlinie 2203
JSON-Richtliniendokument 2204
Weitere Informationen 2208
AWSDeadlineCloud-UserAccessQueues 2208
Diese Richtlinie wird verwendet 2208
Einzelheiten zur Richtlinie 2208
Version der Richtlinie 2208
JSON-Richtliniendokument 2209
Weitere Informationen 2213

AWSDeadlineCloud-WorkerHost 2213
Diese Richtlinie wird verwendet 2214
Einzelheiten zur Richtlinie 2214
Version der Richtlinie 2214
JSON-Richtliniendokument 2214
Weitere Informationen 2215
AWSDeepLensLambdaFunctionAccessPolicy 2216
Diese Richtlinie wird verwendet 2216
Einzelheiten zur Richtlinie 2216
Version der Richtlinie 2216
JSON-Richtliniendokument 2216
Weitere Informationen 2218
AWSDeepLensServiceRolePolicy 2218
Diese Richtlinie wird verwendet 2218
Einzelheiten zur Richtlinie 2218
Version der Richtlinie 2218
JSON-Richtliniendokument 2219
Weitere Informationen 2226
AWSDeepRacerAccountAdminAccess 2226
Diese Richtlinie wird verwendet 2226
Einzelheiten zur Richtlinie 2226
Version der Richtlinie 2226
JSON-Richtliniendokument 2227
Weitere Informationen 2227
AWSDeepRacerCloudFormationAccessPolicy 2227
Diese Richtlinie wird verwendet 2228
Einzelheiten zur Richtlinie 2228
Version der Richtlinie 2228
JSON-Richtliniendokument 2228
Weitere Informationen 2231
AWSDeepRacerDefaultMultiUserAccess 2231
Diese Richtlinie wird verwendet 2231
Einzelheiten zur Richtlinie 2231
Version der Richtlinie 2232
JSON-Richtliniendokument 2232
Weitere Informationen 2233

AWSDeepRacerFullAccess 2234
Diese Richtlinie wird verwendet 2234
Einzelheiten zur Richtlinie 2234
Version der Richtlinie 2234
JSON-Richtliniendokument 2234
Weitere Informationen 2235
AWSDeepRacerRoboMakerAccessPolicy 2235
Diese Richtlinie wird verwendet 2236
Einzelheiten zur Richtlinie 2236
Version der Richtlinie 2236
JSON-Richtliniendokument 2236
Weitere Informationen 2238
AWSDeepRacerServiceRolePolicy 2238
Diese Richtlinie wird verwendet 2238
Einzelheiten zur Richtlinie 2239
Version der Richtlinie 2239
JSON-Richtliniendokument 2239
Weitere Informationen 2242
AWSDenyAll 2242
Diese Richtlinie wird verwendet 2242
Einzelheiten zur Richtlinie 2243
Version der Richtlinie 2243
JSON-Richtliniendokument 2243
Weitere Informationen 2243
AWSDeviceFarmFullAccess 2244
Diese Richtlinie wird verwendet 2244
Einzelheiten zur Richtlinie 2244
Version der Richtlinie 2244
JSON-Richtliniendokument 2244
Weitere Informationen 2245
AWSDeviceFarmServiceRolePolicy 2245
Diese Richtlinie wird verwendet 2245
Einzelheiten der Richtlinie 2245
Version der Richtlinie 2245
JSON-Richtliniendokument 2246
Weitere Informationen 2248

AWSDeviceFarmTestGridServiceRolePolicy 2248
Diese Richtlinie wird verwendet 2248
Einzelheiten der Richtlinie 2248
Version der Richtlinie 2248
JSON-Richtliniendokument 2249
Weitere Informationen 2251
AWSDirectConnectFullAccess 2251
Diese Richtlinie wird verwendet 2251
Einzelheiten zur Richtlinie 2251
Version der Richtlinie 2251
JSON-Richtliniendokument 2252
Weitere Informationen 2252
AWSDirectConnectReadOnlyAccess 2252
Diese Richtlinie wird verwendet 2252
Einzelheiten zur Richtlinie 2253
Version der Richtlinie 2253
JSON-Richtliniendokument 2253
Weitere Informationen 2253
AWSDirectConnectServiceRolePolicy 2254
Diese Richtlinie wird verwendet 2254
Einzelheiten der Richtlinie 2254
Version der Richtlinie 2254
JSON-Richtliniendokument 2254
Weitere Informationen 2255
AWSDirectoryServiceDataFullAccess 2255
Diese Richtlinie wird verwendet 2255
Einzelheiten zur Richtlinie 2255
Version der Richtlinie 2256
JSON-Richtliniendokument 2256
Weitere Informationen 2257
AWSDirectoryServiceDataReadOnlyAccess 2257
Diese Richtlinie wird verwendet 2257
Einzelheiten zur Richtlinie 2257
Version der Richtlinie 2257
JSON-Richtliniendokument 2258
Weitere Informationen 2258

AWSDirectoryServiceFullAccess 2258
Diese Richtlinie wird verwendet 2259
Einzelheiten zur Richtlinie 2259
Version der Richtlinie 2259
JSON-Richtliniendokument 2259
Weitere Informationen 2261
AWSDirectoryServiceReadOnlyAccess 2261
Diese Richtlinie wird verwendet 2261
Einzelheiten zur Richtlinie 2261
Version der Richtlinie 2262
JSON-Richtliniendokument 2262
Weitere Informationen 2262
AWSDirectoryServiceServiceRolePolicy 2263
Diese Richtlinie wird verwendet 2263
Einzelheiten der Richtlinie 2263
Version der Richtlinie 2263
JSON-Richtliniendokument 2263
Weitere Informationen 2265
AWSDiscoveryContinuousExportFirehosePolicy 2265
Diese Richtlinie wird verwendet 2265
Einzelheiten zur Richtlinie 2265
Version der Richtlinie 2265
JSON-Richtliniendokument 2265
Weitere Informationen 2266
AWSDMSFleetAdvisorServiceRolePolicy 2267
Diese Richtlinie wird verwendet 2267
Einzelheiten der Richtlinie 2267
Version der Richtlinie 2267
JSON-Richtliniendokument 2267
Weitere Informationen 2268
AWSDMSServerlessServiceRolePolicy 2268
Diese Richtlinie wird verwendet 2268
Einzelheiten der Richtlinie 2268
Version der Richtlinie 2268
JSON-Richtliniendokument 2269
Weitere Informationen 2271

AWSEC2CapacityManagerServiceRolePolicy 2272
Diese Richtlinie wird verwendet 2272
Einzelheiten der Richtlinie 2272
Version der Richtlinie 2272
JSON-Richtliniendokument 2272
Weitere Informationen 2273
AWSEC2CapacityReservationFleetRolePolicy 2273
Diese Richtlinie wird verwendet 2274
Einzelheiten der Richtlinie 2274
Version der Richtlinie 2274
JSON-Richtliniendokument 2274
Weitere Informationen 2275
AWSEC2FleetServiceRolePolicy 2275
Diese Richtlinie wird verwendet 2276
Einzelheiten der Richtlinie 2276
Version der Richtlinie 2276
JSON-Richtliniendokument 2276
Weitere Informationen 2278
AWSEC2SpotFleetServiceRolePolicy 2278
Diese Richtlinie wird verwendet 2279
Einzelheiten der Richtlinie 2279
Version der Richtlinie 2279
JSON-Richtliniendokument 2279
Weitere Informationen 2281
AWSEC2SpotServiceRolePolicy 2281
Diese Richtlinie wird verwendet 2281
Einzelheiten der Richtlinie 2281
Version der Richtlinie 2282
JSON-Richtliniendokument 2282
Weitere Informationen 2283
AWSEC2SqlHaInstancePolicy 2284
Diese Richtlinie wird verwendet 2284
Einzelheiten zur Richtlinie 2284
Version der Richtlinie 2284
JSON-Richtliniendokument 2284
Weitere Informationen 2286

AWSEC2SqlHaServiceRolePolicy 2286
Diese Richtlinie wird verwendet 2286
Einzelheiten der Richtlinie 2286
Version der Richtlinie 2286
JSON-Richtliniendokument 2287
Weitere Informationen 2288
AWSEC2VssSnapshotPolicy 2289
Diese Richtlinie wird verwendet 2289
Einzelheiten zur Richtlinie 2289
Version der Richtlinie 2289
JSON-Richtliniendokument 2289
Weitere Informationen 2292
AWSECRPullThroughCache_ServiceRolePolicy 2293
Diese Richtlinie wird verwendet 2293
Einzelheiten der Richtlinie 2293
Version der Richtlinie 2293
JSON-Richtliniendokument 2294
Weitere Informationen 2294
AWSElasticBeanstalkCustomPlatformforEC2Role 2295
Diese Richtlinie wird verwendet 2295
Einzelheiten zur Richtlinie 2295
Version der Richtlinie 2295
JSON-Richtliniendokument 2295
Weitere Informationen 2297
AWSElasticBeanstalkEnhancedHealth 2297
Diese Richtlinie wird verwendet 2297
Einzelheiten zur Richtlinie 2298
Version der Richtlinie 2298
JSON-Richtliniendokument 2298
Weitere Informationen 2299
AWSElasticBeanstalkMaintenance 2299
Diese Richtlinie wird verwendet 2299
Einzelheiten der Richtlinie 2300
Version der Richtlinie 2300
JSON-Richtliniendokument 2300
Weitere Informationen 2301

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy 2301
Diese Richtlinie wird verwendet 2301
Einzelheiten zur Richtlinie 2301
Version der Richtlinie 2302
JSON-Richtliniendokument 2302
Weitere Informationen 2309
AWSElasticBeanstalkManagedUpdatesServiceRolePolicy 2309
Diese Richtlinie wird verwendet 2309
Einzelheiten der Richtlinie 2309
Version der Richtlinie 2310
JSON-Richtliniendokument 2310
Weitere Informationen 2315
AWSElasticBeanstalkMulticontainerDocker 2315
Diese Richtlinie wird verwendet 2316
Einzelheiten zur Richtlinie 2316
Version der Richtlinie 2316
JSON-Richtliniendokument 2316
Weitere Informationen 2317
AWSElasticBeanstalkReadOnly 2317
Diese Richtlinie wird verwendet 2318
Einzelheiten zur Richtlinie 2318
Version der Richtlinie 2318
JSON-Richtliniendokument 2318
Weitere Informationen 2320
AWSElasticBeanstalkRoleCore 2320
Diese Richtlinie wird verwendet 2321
Einzelheiten zur Richtlinie 2321
Version der Richtlinie 2321
JSON-Richtliniendokument 2321
Weitere Informationen 2326
AWSElasticBeanstalkRoleCWL 2326
Diese Richtlinie wird verwendet 2326
Einzelheiten zur Richtlinie 2326
Version der Richtlinie 2327
JSON-Richtliniendokument 2327
Weitere Informationen 2327

AWSElasticBeanstalkRoleECS 2328
Diese Richtlinie wird verwendet 2328
Einzelheiten zur Richtlinie 2328
Version der Richtlinie 2328
JSON-Richtliniendokument 2328
Weitere Informationen 2329
AWSElasticBeanstalkRoleRDS 2329
Diese Richtlinie wird verwendet 2330
Einzelheiten zur Richtlinie 2330
Version der Richtlinie 2330
JSON-Richtliniendokument 2330
Weitere Informationen 2331
AWSElasticBeanstalkRoleSNS 2331
Diese Richtlinie wird verwendet 2331
Einzelheiten zur Richtlinie 2331
Version der Richtlinie 2331
JSON-Richtliniendokument 2332
Weitere Informationen 2332
AWSElasticBeanstalkRoleWorkerTier 2333
Diese Richtlinie wird verwendet 2333
Einzelheiten zur Richtlinie 2333
Version der Richtlinie 2333
JSON-Richtliniendokument 2333
Weitere Informationen 2334
AWSElasticBeanstalkService 2334
Diese Richtlinie wird verwendet 2334
Einzelheiten zur Richtlinie 2335
Version der Richtlinie 2335
JSON-Richtliniendokument 2335
Weitere Informationen 2339
AWSElasticBeanstalkServiceRolePolicy 2340
Diese Richtlinie wird verwendet 2340
Einzelheiten der Richtlinie 2340
Version der Richtlinie 2340
JSON-Richtliniendokument 2340
Weitere Informationen 2342

AWSElasticBeanstalkWebTier 2342
Diese Richtlinie wird verwendet 2342
Einzelheiten zur Richtlinie 2342
Version der Richtlinie 2342
JSON-Richtliniendokument 2343
Weitere Informationen 2344
AWSElasticBeanstalkWorkerTier 2344
Diese Richtlinie wird verwendet 2344
Einzelheiten zur Richtlinie 2345
Version der Richtlinie 2345
JSON-Richtliniendokument 2345
Weitere Informationen 2347
AWSElasticDisasterRecoveryAgentInstallationPolicy 2347
Diese Richtlinie wird verwendet 2348
Einzelheiten zur Richtlinie 2348
Version der Richtlinie 2348
JSON-Richtliniendokument 2348
Weitere Informationen 2350
AWSElasticDisasterRecoveryAgentPolicy 2350
Diese Richtlinie wird verwendet 2350
Einzelheiten zur Richtlinie 2350
Version der Richtlinie 2350
JSON-Richtliniendokument 2351
Weitere Informationen 2351
AWSElasticDisasterRecoveryConsoleFullAccess 2352
Diese Richtlinie wird verwendet 2352
Einzelheiten zur Richtlinie 2352
Version der Richtlinie 2352
JSON-Richtliniendokument 2352
Weitere Informationen 2362
AWSElasticDisasterRecoveryConsoleFullAccess_v2 2363
Diese Richtlinie wird verwendet 2363
Einzelheiten zur Richtlinie 2363
Version der Richtlinie 2363
JSON-Richtliniendokument 2364
Weitere Informationen 2379

AWSElasticDisasterRecoveryConversionServerPolicy 2379
Diese Richtlinie wird verwendet 2380
Einzelheiten zur Richtlinie 2380
Version der Richtlinie 2380
JSON-Richtliniendokument 2380
Weitere Informationen 2381
AWSElasticDisasterRecoveryCrossAccountReplicationPolicy 2381
Diese Richtlinie wird verwendet 2381
Einzelheiten zur Richtlinie 2381
Version der Richtlinie 2382
JSON-Richtliniendokument 2382
Weitere Informationen 2383
AWSElasticDisasterRecoveryEc2InstancePolicy 2383
Diese Richtlinie wird verwendet 2383
Einzelheiten zur Richtlinie 2383
Version der Richtlinie 2383
JSON-Richtliniendokument 2384
Weitere Informationen 2386
AWSElasticDisasterRecoveryFailbackInstallationPolicy 2386
Diese Richtlinie wird verwendet 2386
Einzelheiten zur Richtlinie 2386
Version der Richtlinie 2386
JSON-Richtliniendokument 2387
Weitere Informationen 2387
AWSElasticDisasterRecoveryFailbackPolicy 2388
Diese Richtlinie wird verwendet 2388
Einzelheiten zur Richtlinie 2388
Version der Richtlinie 2388
JSON-Richtliniendokument 2389
Weitere Informationen 2390
AWSElasticDisasterRecoveryLaunchActionsPolicy 2390
Diese Richtlinie wird verwendet 2390
Einzelheiten zur Richtlinie 2390
Version der Richtlinie 2391
JSON-Richtliniendokument 2391
Weitere Informationen 2397

AWSElasticDisasterRecoveryNetworkReplicationPolicy 2397
Diese Richtlinie wird verwendet 2397
Einzelheiten zur Richtlinie 2397
Version der Richtlinie 2398
JSON-Richtliniendokument 2398
Weitere Informationen 2398
AWSElasticDisasterRecoveryReadOnlyAccess 2399
Diese Richtlinie wird verwendet 2399
Einzelheiten zur Richtlinie 2399
Version der Richtlinie 2399
JSON-Richtliniendokument 2400
Weitere Informationen 2402
AWSElasticDisasterRecoveryRecoveryInstancePolicy 2402
Diese Richtlinie wird verwendet 2402
Einzelheiten zur Richtlinie 2402
Version der Richtlinie 2403
JSON-Richtliniendokument 2403
Weitere Informationen 2405
AWSElasticDisasterRecoveryReplicationServerPolicy 2406
Diese Richtlinie wird verwendet 2406
Einzelheiten zur Richtlinie 2406
Version der Richtlinie 2406
JSON-Richtliniendokument 2407
Weitere Informationen 2409
AWSElasticDisasterRecoveryServiceRolePolicy 2409
Diese Richtlinie wird verwendet 2409
Einzelheiten der Richtlinie 2409
Version der Richtlinie 2409
JSON-Richtliniendokument 2410
Weitere Informationen 2420
AWSElasticDisasterRecoveryStagingAccountPolicy 2420
Diese Richtlinie wird verwendet 2420
Einzelheiten zur Richtlinie 2420
Version der Richtlinie 2420
JSON-Richtliniendokument 2421
Weitere Informationen 2422

AWSElasticDisasterRecoveryStagingAccountPolicy_v2 2422
Diese Richtlinie wird verwendet 2422
Einzelheiten zur Richtlinie 2422
Version der Richtlinie 2422
JSON-Richtliniendokument 2423
Weitere Informationen 2424
AWSElasticLoadBalancingClassicServiceRolePolicy 2424
Diese Richtlinie wird verwendet 2424
Einzelheiten der Richtlinie 2424
Version der Richtlinie 2424
JSON-Richtliniendokument 2425
Weitere Informationen 2426
AWSElasticLoadBalancingServiceRolePolicy 2426
Diese Richtlinie wird verwendet 2426
Einzelheiten der Richtlinie 2426
Version der Richtlinie 2426
JSON-Richtliniendokument 2427
Weitere Informationen 2428
AWSElementalMediaConnectFullAccess 2428
Diese Richtlinie wird verwendet 2428
Einzelheiten zur Richtlinie 2428
Version der Richtlinie 2428
JSON-Richtliniendokument 2429
Weitere Informationen 2429
AWSElementalMediaConnectReadOnlyAccess 2429
Diese Richtlinie wird verwendet 2429
Einzelheiten zur Richtlinie 2430
Version der Richtlinie 2430
JSON-Richtliniendokument 2430
Weitere Informationen 2431
AWSElementalMediaConvertFullAccess 2431
Diese Richtlinie wird verwendet 2431
Einzelheiten zur Richtlinie 2431
Version der Richtlinie 2431
JSON-Richtliniendokument 2432
Weitere Informationen 2432

AWSElementalMediaConvertReadOnly 2433
Diese Richtlinie wird verwendet 2433
Einzelheiten zur Richtlinie 2433
Version der Richtlinie 2433
JSON-Richtliniendokument 2433
Weitere Informationen 2434
AWSElementalMediaLiveFullAccess 2434
Diese Richtlinie wird verwendet 2434
Einzelheiten zur Richtlinie 2434
Version der Richtlinie 2435
JSON-Richtliniendokument 2435
Weitere Informationen 2435
AWSElementalMediaLiveReadOnly 2435
Diese Richtlinie wird verwendet 2435
Einzelheiten zur Richtlinie 2436
Version der Richtlinie 2436
JSON-Richtliniendokument 2436
Weitere Informationen 2436
AWSElementalMediaPackageFullAccess 2437
Diese Richtlinie wird verwendet 2437
Einzelheiten zur Richtlinie 2437
Version der Richtlinie 2437
JSON-Richtliniendokument 2437
Weitere Informationen 2438
AWSElementalMediaPackageReadOnly 2438
Diese Richtlinie wird verwendet 2438
Einzelheiten zur Richtlinie 2438
Version der Richtlinie 2438
JSON-Richtliniendokument 2439
Weitere Informationen 2439
AWSElementalMediaPackageV2FullAccess 2439
Diese Richtlinie wird verwendet 2439
Einzelheiten zur Richtlinie 2439
Version der Richtlinie 2440
JSON-Richtliniendokument 2440
Weitere Informationen 2440

AWSElementalMediaPackageV2ReadOnly 2440
Diese Richtlinie wird verwendet 2441
Einzelheiten zur Richtlinie 2441
Version der Richtlinie 2441
JSON-Richtliniendokument 2441
Weitere Informationen 2441
AWSElementalMediaStoreFullAccess 2442
Diese Richtlinie wird verwendet 2442
Einzelheiten zur Richtlinie 2442
Version der Richtlinie 2442
JSON-Richtliniendokument 2442
Weitere Informationen 2443
AWSElementalMediaStoreReadOnly 2443
Diese Richtlinie wird verwendet 2443
Einzelheiten zur Richtlinie 2443
Version der Richtlinie 2444
JSON-Richtliniendokument 2444
Weitere Informationen 2444
AWSElementalMediaTailorFullAccess 2445
Diese Richtlinie wird verwendet 2445
Einzelheiten zur Richtlinie 2445
Version der Richtlinie 2445
JSON-Richtliniendokument 2445
Weitere Informationen 2446
AWSElementalMediaTailorReadOnly 2446
Diese Richtlinie wird verwendet 2446
Einzelheiten zur Richtlinie 2446
Version der Richtlinie 2446
JSON-Richtliniendokument 2447
Weitere Informationen 2447
AWSEnhancedClassicNetworkingMangementPolicy 2447
Diese Richtlinie wird verwendet 2447
Einzelheiten der Richtlinie 2447
Version der Richtlinie 2448
JSON-Richtliniendokument 2448
Weitere Informationen 2448

AWSEntityResolutionConsoleFullAccess 2448
Diese Richtlinie wird verwendet 2449
Einzelheiten zur Richtlinie 2449
Version der Richtlinie 2449
JSON-Richtliniendokument 2449
Weitere Informationen 2452
AWSEntityResolutionConsoleReadOnlyAccess 2453
Diese Richtlinie wird verwendet 2453
Einzelheiten zur Richtlinie 2453
Version der Richtlinie 2453
JSON-Richtliniendokument 2453
Weitere Informationen 2454
AWSFaultInjectionSimulatorEC2Access 2454
Diese Richtlinie wird verwendet 2454
Einzelheiten zur Richtlinie 2454
Version der Richtlinie 2454
JSON-Richtliniendokument 2455
Weitere Informationen 2456
AWSFaultInjectionSimulatorECSAccess 2457
Diese Richtlinie wird verwendet 2457
Einzelheiten zur Richtlinie 2457
Version der Richtlinie 2457
JSON-Richtliniendokument 2457
Weitere Informationen 2459
AWSFaultInjectionSimulatorEKSAccess 2460
Diese Richtlinie wird verwendet 2460
Einzelheiten zur Richtlinie 2460
Version der Richtlinie 2460
JSON-Richtliniendokument 2460
Weitere Informationen 2462
AWSFaultInjectionSimulatorNetworkAccess 2462
Diese Richtlinie wird verwendet 2462
Einzelheiten zur Richtlinie 2462
Version der Richtlinie 2462
JSON-Richtliniendokument 2463
Weitere Informationen 2469

AWSFaultInjectionSimulatorRDSAccess 2470
Diese Richtlinie wird verwendet 2470
Einzelheiten zur Richtlinie 2470
Version der Richtlinie 2470
JSON-Richtliniendokument 2470
Weitere Informationen 2471
AWSFaultInjectionSimulatorSSMAccess 2472
Diese Richtlinie wird verwendet 2472
Einzelheiten zur Richtlinie 2472
Version der Richtlinie 2472
JSON-Richtliniendokument 2472
Weitere Informationen 2474
AWSFinSpaceServiceRolePolicy 2474
Diese Richtlinie wird verwendet 2474
Einzelheiten der Richtlinie 2474
Version der Richtlinie 2475
JSON-Richtliniendokument 2475
Weitere Informationen 2475
AWSFMAdminFullAccess 2475
Diese Richtlinie wird verwendet 2476
Einzelheiten zur Richtlinie 2476
Version der Richtlinie 2476
JSON-Richtliniendokument 2476
Weitere Informationen 2478
AWSFMAdminReadOnlyAccess 2478
Diese Richtlinie wird verwendet 2478
Einzelheiten zur Richtlinie 2478
Version der Richtlinie 2479
JSON-Richtliniendokument 2479
Weitere Informationen 2480
AWSFMMemberReadOnlyAccess 2481
Diese Richtlinie wird verwendet 2481
Einzelheiten zur Richtlinie 2481
Version der Richtlinie 2481
JSON-Richtliniendokument 2481
Weitere Informationen 2482

AWSForWordPressPluginPolicy 2482
Diese Richtlinie wird verwendet 2482
Einzelheiten zur Richtlinie 2482
Version der Richtlinie 2482
JSON-Richtliniendokument 2483
Weitere Informationen 2484
AWSGitSyncServiceRolePolicy 2485
Diese Richtlinie wird verwendet 2485
Einzelheiten der Richtlinie 2485
Version der Richtlinie 2485
JSON-Richtliniendokument 2485
Weitere Informationen 2486
AWSGlobalAcceleratorSLRPolicy 2486
Diese Richtlinie wird verwendet 2486
Einzelheiten der Richtlinie 2487
Version der Richtlinie 2487
JSON-Richtliniendokument 2487
Weitere Informationen 2489
AWSGlueConsoleFullAccess 2489
Diese Richtlinie wird verwendet 2489
Einzelheiten zur Richtlinie 2489
Version der Richtlinie 2489
JSON-Richtliniendokument 2489
Weitere Informationen 2494
AWSGlueConsoleSageMakerNotebookFullAccess 2494
Diese Richtlinie wird verwendet 2494
Einzelheiten zur Richtlinie 2494
Version der Richtlinie 2494
JSON-Richtliniendokument 2495
Weitere Informationen 2500
AwsGlueDataBrewFullAccessPolicy 2500
Diese Richtlinie wird verwendet 2500
Einzelheiten zur Richtlinie 2500
Version der Richtlinie 2500
JSON-Richtliniendokument 2501
Weitere Informationen 2506

AWSGlueDataBrewServiceRole 2506
Diese Richtlinie wird verwendet 2506
Einzelheiten zur Richtlinie 2506
Version der Richtlinie 2507
JSON-Richtliniendokument 2507
Weitere Informationen 2510
AWSGlueSchemaRegistryFullAccess 2510
Diese Richtlinie wird verwendet 2510
Einzelheiten zur Richtlinie 2510
Version der Richtlinie 2510
JSON-Richtliniendokument 2511
Weitere Informationen 2512
AWSGlueSchemaRegistryReadonlyAccess 2512
Diese Richtlinie wird verwendet 2512
Einzelheiten zur Richtlinie 2512
Version der Richtlinie 2512
JSON-Richtliniendokument 2513
Weitere Informationen 2513
AWSGlueServiceNotebookRole 2514
Diese Richtlinie wird verwendet 2514
Einzelheiten zur Richtlinie 2514
Version der Richtlinie 2514
JSON-Richtliniendokument 2514
Weitere Informationen 2517
AWSGlueServiceRole 2517
Diese Richtlinie wird verwendet 2517
Einzelheiten zur Richtlinie 2517
Version der Richtlinie 2517
JSON-Richtliniendokument 2518
Weitere Informationen 2520
AwsGlueSessionUserRestrictedNotebookPolicy 2520
Diese Richtlinie wird verwendet 2520
Einzelheiten zur Richtlinie 2520
Version der Richtlinie 2521
JSON-Richtliniendokument 2521
Weitere Informationen 2524

AwsGlueSessionUserRestrictedNotebookServiceRole 2524
Diese Richtlinie wird verwendet 2524
Einzelheiten zur Richtlinie 2524
Version der Richtlinie 2524
JSON-Richtliniendokument 2525
Weitere Informationen 2528
AwsGlueSessionUserRestrictedPolicy 2529
Diese Richtlinie wird verwendet 2529
Einzelheiten zur Richtlinie 2529
Version der Richtlinie 2529
JSON-Richtliniendokument 2530
Weitere Informationen 2532
AwsGlueSessionUserRestrictedServiceRole 2533
Diese Richtlinie wird verwendet 2533
Einzelheiten zur Richtlinie 2533
Version der Richtlinie 2533
JSON-Richtliniendokument 2533
Weitere Informationen 2538
AWSGrafanaAccountAdministrator 2538
Diese Richtlinie wird verwendet 2538
Einzelheiten zur Richtlinie 2538
Version der Richtlinie 2538
JSON-Richtliniendokument 2539
Weitere Informationen 2540
AWSGrafanaConsoleReadOnlyAccess 2540
Diese Richtlinie wird verwendet 2540
Einzelheiten zur Richtlinie 2540
Version der Richtlinie 2540
JSON-Richtliniendokument 2541
Weitere Informationen 2541
AWSGrafanaWorkspacePermissionManagement 2541
Diese Richtlinie wird verwendet 2541
Einzelheiten zur Richtlinie 2542
Version der Richtlinie 2542
JSON-Richtliniendokument 2542
Weitere Informationen 2543

AWSGrafanaWorkspacePermissionManagementV2 2543
Diese Richtlinie wird verwendet 2543
Einzelheiten zur Richtlinie 2543
Version der Richtlinie 2544
JSON-Richtliniendokument 2544
Weitere Informationen 2545
AWSGreengrassFullAccess 2545
Diese Richtlinie wird verwendet 2545
Einzelheiten zur Richtlinie 2545
Version der Richtlinie 2545
JSON-Richtliniendokument 2546
Weitere Informationen 2546
AWSGreengrassReadOnlyAccess 2546
Diese Richtlinie wird verwendet 2546
Einzelheiten zur Richtlinie 2547
Version der Richtlinie 2547
JSON-Richtliniendokument 2547
Weitere Informationen 2547
AWSGreengrassResourceAccessRolePolicy 2548
Diese Richtlinie wird verwendet 2548
Einzelheiten zur Richtlinie 2548
Version der Richtlinie 2548
JSON-Richtliniendokument 2548
Weitere Informationen 2551
AWSGroundStationAgentInstancePolicy 2551
Diese Richtlinie wird verwendet 2551
Einzelheiten zur Richtlinie 2551
Version der Richtlinie 2551
JSON-Richtliniendokument 2552
Weitere Informationen 2552
AWSHealth_EventProcessorServiceRolePolicy 2552
Diese Richtlinie wird verwendet 2553
Einzelheiten der Richtlinie 2553
Version der Richtlinie 2553
JSON-Richtliniendokument 2553
Weitere Informationen 2554

AWSHealthFullAccess 2554
Diese Richtlinie wird verwendet 2554
Einzelheiten zur Richtlinie 2554
Version der Richtlinie 2555
JSON-Richtliniendokument 2555
Weitere Informationen 2556
AWSHealthImagingFullAccess 2556
Diese Richtlinie wird verwendet 2556
Einzelheiten zur Richtlinie 2556
Version der Richtlinie 2556
JSON-Richtliniendokument 2557
Weitere Informationen 2557
AWSHealthImagingReadOnlyAccess 2558
Diese Richtlinie wird verwendet 2558
Einzelheiten zur Richtlinie 2558
Version der Richtlinie 2558
JSON-Richtliniendokument 2558
Weitere Informationen 2559
AWSIAMIdentityCenterAllowListForIdentityContext 2559
Diese Richtlinie wird verwendet 2559
Einzelheiten zur Richtlinie 2559
Version der Richtlinie 2560
JSON-Richtliniendokument 2560
Weitere Informationen 2563
AWSIdentityCenterExternalManagementPolicy 2563
Diese Richtlinie wird verwendet 2563
Einzelheiten zur Richtlinie 2563
Version der Richtlinie 2564
JSON-Richtliniendokument 2564
Weitere Informationen 2566
AWSIdentitySyncFullAccess 2566
Diese Richtlinie wird verwendet 2566
Einzelheiten zur Richtlinie 2566
Version der Richtlinie 2566
JSON-Richtliniendokument 2567
Weitere Informationen 2567

AWSIdentitySyncReadOnlyAccess 2568
Diese Richtlinie wird verwendet 2568
Einzelheiten zur Richtlinie 2568
Version der Richtlinie 2568
JSON-Richtliniendokument 2568
Weitere Informationen 2569
AWSImageBuilderFullAccess 2569
Diese Richtlinie wird verwendet 2569
Einzelheiten zur Richtlinie 2569
Version der Richtlinie 2569
JSON-Richtliniendokument 2570
Weitere Informationen 2572
AWSImageBuilderReadOnlyAccess 2572
Diese Richtlinie wird verwendet 2573
Einzelheiten zur Richtlinie 2573
Version der Richtlinie 2573
JSON-Richtliniendokument 2573
Weitere Informationen 2574
AWSImportExportFullAccess 2574
Diese Richtlinie wird verwendet 2574
Einzelheiten zur Richtlinie 2574
Version der Richtlinie 2574
JSON-Richtliniendokument 2575
Weitere Informationen 2575
AWSImportExportReadOnlyAccess 2575
Diese Richtlinie wird verwendet 2575
Einzelheiten zur Richtlinie 2576
Version der Richtlinie 2576
JSON-Richtliniendokument 2576
Weitere Informationen 2576
AWSIncidentManagerIncidentAccessServiceRolePolicy 2577
Diese Richtlinie wird verwendet 2577
Einzelheiten zur Richtlinie 2577
Version der Richtlinie 2577
JSON-Richtliniendokument 2577
Weitere Informationen 2578

AWSIncidentManagerResolverAccess 2578
Diese Richtlinie wird verwendet 2578
Einzelheiten zur Richtlinie 2578
Version der Richtlinie 2579
JSON-Richtliniendokument 2579
Weitere Informationen 2580
AWSIncidentManagerServiceRolePolicy 2580
Diese Richtlinie wird verwendet 2580
Einzelheiten der Richtlinie 2580
Version der Richtlinie 2581
JSON-Richtliniendokument 2581
Weitere Informationen 2582
AWSIoT1ClickFullAccess 2582
Diese Richtlinie wird verwendet 2582
Einzelheiten zur Richtlinie 2582
Version der Richtlinie 2583
JSON-Richtliniendokument 2583
Weitere Informationen 2583
AWSIoT1ClickReadOnlyAccess 2583
Diese Richtlinie wird verwendet 2584
Einzelheiten zur Richtlinie 2584
Version der Richtlinie 2584
JSON-Richtliniendokument 2584
Weitere Informationen 2585
AWSIoTAnalyticsFullAccess 2585
Diese Richtlinie wird verwendet 2585
Einzelheiten zur Richtlinie 2585
Version der Richtlinie 2585
JSON-Richtliniendokument 2585
Weitere Informationen 2586
AWSIoTAnalyticsReadOnlyAccess 2586
Diese Richtlinie wird verwendet 2586
Einzelheiten zur Richtlinie 2586
Version der Richtlinie 2587
JSON-Richtliniendokument 2587
Weitere Informationen 2587

AWSIoTConfigAccess 2587
Diese Richtlinie wird verwendet 2588
Einzelheiten zur Richtlinie 2588
Version der Richtlinie 2588
JSON-Richtliniendokument 2588
Weitere Informationen 2592
AWSIoTConfigReadOnlyAccess 2592
Diese Richtlinie wird verwendet 2592
Einzelheiten zur Richtlinie 2592
Version der Richtlinie 2593
JSON-Richtliniendokument 2593
Weitere Informationen 2595
AWSIoTDataAccess 2595
Diese Richtlinie wird verwendet 2595
Einzelheiten zur Richtlinie 2595
Version der Richtlinie 2595
JSON-Richtliniendokument 2596
Weitere Informationen 2596
AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction 2596
Diese Richtlinie wird verwendet 2597
Einzelheiten zur Richtlinie 2597
Version der Richtlinie 2597
JSON-Richtliniendokument 2597
Weitere Informationen 2598
AWSIoTDeviceDefenderAudit 2598
Diese Richtlinie wird verwendet 2598
Einzelheiten zur Richtlinie 2598
Version der Richtlinie 2598
JSON-Richtliniendokument 2599
Weitere Informationen 2599
AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction 2600
Diese Richtlinie wird verwendet 2600
Einzelheiten zur Richtlinie 2600
Version der Richtlinie 2600
JSON-Richtliniendokument 2601
Weitere Informationen 2601

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction 2602
Diese Richtlinie wird verwendet 2602
Einzelheiten zur Richtlinie 2602
Version der Richtlinie 2602
JSON-Richtliniendokument 2602
Weitere Informationen 2603
AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction 2603
Diese Richtlinie wird verwendet 2603
Einzelheiten zur Richtlinie 2603
Version der Richtlinie 2604
JSON-Richtliniendokument 2604
Weitere Informationen 2604
AWSIoTDeviceDefenderUpdateCACertMitigationAction 2604
Diese Richtlinie wird verwendet 2605
Einzelheiten zur Richtlinie 2605
Version der Richtlinie 2605
JSON-Richtliniendokument 2605
Weitere Informationen 2606
AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction 2606
Diese Richtlinie wird verwendet 2606
Einzelheiten zur Richtlinie 2606
Version der Richtlinie 2606
JSON-Richtliniendokument 2607
Weitere Informationen 2607
AWSIoTDeviceTesterForFreeRTOSFullAccess 2607
Diese Richtlinie wird verwendet 2607
Einzelheiten zur Richtlinie 2608
Version der Richtlinie 2608
JSON-Richtliniendokument 2608
Weitere Informationen 2614
AWSIoTDeviceTesterForGreengrassFullAccess 2614
Diese Richtlinie wird verwendet 2615
Einzelheiten zur Richtlinie 2615
Version der Richtlinie 2615
JSON-Richtliniendokument 2615
Weitere Informationen 2618

AWSIoTEventsFullAccess 2618
Diese Richtlinie wird verwendet 2618
Einzelheiten zur Richtlinie 2618
Version der Richtlinie 2619
JSON-Richtliniendokument 2619
Weitere Informationen 2619
AWSIoTEventsReadOnlyAccess 2619
Diese Richtlinie wird verwendet 2620
Einzelheiten zur Richtlinie 2620
Version der Richtlinie 2620
JSON-Richtliniendokument 2620
Weitere Informationen 2621
AWSIoTFleetHubFederationAccess 2621
Diese Richtlinie wird verwendet 2621
Einzelheiten zur Richtlinie 2621
Version der Richtlinie 2621
JSON-Richtliniendokument 2621
Weitere Informationen 2623
AWSIoTFleetwiseServiceRolePolicy 2623
Diese Richtlinie wird verwendet 2624
Einzelheiten der Richtlinie 2624
Version der Richtlinie 2624
JSON-Richtliniendokument 2624
Weitere Informationen 2625
AWSIoTFullAccess 2625
Diese Richtlinie wird verwendet 2625
Einzelheiten zur Richtlinie 2625
Version der Richtlinie 2625
JSON-Richtliniendokument 2626
Weitere Informationen 2626
AWSIoTLogging 2626
Diese Richtlinie wird verwendet 2626
Einzelheiten zur Richtlinie 2627
Version der Richtlinie 2627
JSON-Richtliniendokument 2627
Weitere Informationen 2628

AWSIoTManagedIntegrationsFullAccess 2628
Diese Richtlinie wird verwendet 2628
Einzelheiten zur Richtlinie 2628
Version der Richtlinie 2628
JSON-Richtliniendokument 2629
Weitere Informationen 2629
AWSIoTManagedIntegrationsRolePolicy 2629
Diese Richtlinie wird verwendet 2630
Einzelheiten der Richtlinie 2630
Version der Richtlinie 2630
JSON-Richtliniendokument 2630
Weitere Informationen 2631
AWSIoTOTAUpdate 2632
Diese Richtlinie wird verwendet 2632
Einzelheiten zur Richtlinie 2632
Version der Richtlinie 2632
JSON-Richtliniendokument 2632
Weitere Informationen 2633
AWSIotRoboRunnerFullAccess 2633
Diese Richtlinie wird verwendet 2633
Einzelheiten zur Richtlinie 2633
Version der Richtlinie 2633
JSON-Richtliniendokument 2634
Weitere Informationen 2634
AWSIotRoboRunnerReadOnly 2634
Diese Richtlinie wird verwendet 2635
Einzelheiten zur Richtlinie 2635
Version der Richtlinie 2635
JSON-Richtliniendokument 2635
Weitere Informationen 2636
AWSIotRoboRunnerServiceRolePolicy 2636
Diese Richtlinie wird verwendet 2636
Einzelheiten der Richtlinie 2636
Version der Richtlinie 2636
JSON-Richtliniendokument 2637
Weitere Informationen 2637

AWSIoTRuleActions 2637
Diese Richtlinie wird verwendet 2638
Einzelheiten zur Richtlinie 2638
Version der Richtlinie 2638
JSON-Richtliniendokument 2638
Weitere Informationen 2639
AWSIoTSiteWiseConsoleFullAccess 2639
Diese Richtlinie wird verwendet 2639
Einzelheiten zur Richtlinie 2639
Version der Richtlinie 2640
JSON-Richtliniendokument 2640
Weitere Informationen 2642
AWSIoTSiteWiseFullAccess 2642
Diese Richtlinie wird verwendet 2642
Einzelheiten zur Richtlinie 2642
Version der Richtlinie 2643
JSON-Richtliniendokument 2643
Weitere Informationen 2643
AWSIoTSiteWiseMonitorPortalAccess 2643
Diese Richtlinie wird verwendet 2644
Einzelheiten zur Richtlinie 2644
Version der Richtlinie 2644
JSON-Richtliniendokument 2644
Weitere Informationen 2645
AWSIoTSiteWiseMonitorServiceRolePolicy 2645
Diese Richtlinie wird verwendet 2646
Einzelheiten der Richtlinie 2646
Version der Richtlinie 2646
JSON-Richtliniendokument 2646
Weitere Informationen 2647
AWSIoTSiteWiseReadOnlyAccess 2647
Diese Richtlinie wird verwendet 2647
Einzelheiten zur Richtlinie 2648
Version der Richtlinie 2648
JSON-Richtliniendokument 2648
Weitere Informationen 2650

AWSIoTThingsRegistration 2650
Diese Richtlinie wird verwendet 2650
Einzelheiten zur Richtlinie 2650
Version der Richtlinie 2650
JSON-Richtliniendokument 2651
Weitere Informationen 2652
AWSIoTTwinMakerServiceRolePolicy 2652
Diese Richtlinie wird verwendet 2652
Einzelheiten der Richtlinie 2652
Version der Richtlinie 2652
JSON-Richtliniendokument 2653
Weitere Informationen 2654
AWSIoTWirelessDataAccess 2654
Diese Richtlinie wird verwendet 2655
Einzelheiten zur Richtlinie 2655
Version der Richtlinie 2655
JSON-Richtliniendokument 2655
Weitere Informationen 2655
AWSIoTWirelessFullAccess 2656
Diese Richtlinie wird verwendet 2656
Einzelheiten zur Richtlinie 2656
Version der Richtlinie 2656
JSON-Richtliniendokument 2656
Weitere Informationen 2657
AWSIoTWirelessFullPublishAccess 2657
Diese Richtlinie wird verwendet 2657
Einzelheiten zur Richtlinie 2657
Version der Richtlinie 2658
JSON-Richtliniendokument 2658
Weitere Informationen 2658
AWSIoTWirelessGatewayCertManager 2658
Diese Richtlinie wird verwendet 2659
Einzelheiten zur Richtlinie 2659
Version der Richtlinie 2659
JSON-Richtliniendokument 2659
Weitere Informationen 2660

AWSIoTWirelessLogging 2660
Diese Richtlinie wird verwendet 2660
Einzelheiten zur Richtlinie 2660
Version der Richtlinie 2660
JSON-Richtliniendokument 2661
Weitere Informationen 2661
AWSIoTWirelessReadOnlyAccess 2661
Diese Richtlinie wird verwendet 2661
Einzelheiten zur Richtlinie 2662
Version der Richtlinie 2662
JSON-Richtliniendokument 2662
Weitere Informationen 2662
AWSIPAMServiceRolePolicy 2663
Diese Richtlinie wird verwendet 2663
Einzelheiten der Richtlinie 2663
Version der Richtlinie 2663
JSON-Richtliniendokument 2663
Weitere Informationen 2665
AWSIQContractServiceRolePolicy 2666
Diese Richtlinie wird verwendet 2666
Einzelheiten der Richtlinie 2666
Version der Richtlinie 2666
JSON-Richtliniendokument 2666
Weitere Informationen 2667
AWSIQFullAccess 2667
Diese Richtlinie wird verwendet 2667
Einzelheiten zur Richtlinie 2667
Version der Richtlinie 2667
JSON-Richtliniendokument 2668
Weitere Informationen 2668
AWSIQPermissionServiceRolePolicy 2668
Diese Richtlinie wird verwendet 2669
Einzelheiten der Richtlinie 2669
Version der Richtlinie 2669
JSON-Richtliniendokument 2669
Weitere Informationen 2670

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy 2670
Diese Richtlinie wird verwendet 2670
Einzelheiten der Richtlinie 2671
Version der Richtlinie 2671
JSON-Richtliniendokument 2671
Weitere Informationen 2672
AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy 2672
Diese Richtlinie wird verwendet 2672
Einzelheiten der Richtlinie 2672
Version der Richtlinie 2672
JSON-Richtliniendokument 2673
Weitere Informationen 2673
AWSKeyManagementServicePowerUser 2673
Diese Richtlinie wird verwendet 2673
Einzelheiten zur Richtlinie 2673
Version der Richtlinie 2674
JSON-Richtliniendokument 2674
Weitere Informationen 2674
AWSLakeFormationCrossAccountManager 2675
Diese Richtlinie wird verwendet 2675
Einzelheiten zur Richtlinie 2675
Version der Richtlinie 2675
JSON-Richtliniendokument 2675
Weitere Informationen 2677
AWSLakeFormationDataAdmin 2678
Diese Richtlinie wird verwendet 2678
Einzelheiten zur Richtlinie 2678
Version der Richtlinie 2678
JSON-Richtliniendokument 2678
Weitere Informationen 2680
AWSLambda_FullAccess 2680
Diese Richtlinie wird verwendet 2680
Einzelheiten zur Richtlinie 2680
Version der Richtlinie 2680
JSON-Richtliniendokument 2681
Weitere Informationen 2682

AWSLambda_ReadOnlyAccess 2682
Diese Richtlinie wird verwendet 2683
Einzelheiten zur Richtlinie 2683
Version der Richtlinie 2683
JSON-Richtliniendokument 2683
Weitere Informationen 2684
AWSLambdaBasicDurableExecutionRolePolicy 2685
Diese Richtlinie wird verwendet 2685
Einzelheiten zur Richtlinie 2685
Version der Richtlinie 2685
JSON-Richtliniendokument 2685
Weitere Informationen 2686
AWSLambdaBasicExecutionRole 2686
Diese Richtlinie wird verwendet 2686
Einzelheiten zur Richtlinie 2686
Version der Richtlinie 2686
JSON-Richtliniendokument 2687
Weitere Informationen 2687
AWSLambdaDynamoDBExecutionRole 2687
Diese Richtlinie wird verwendet 2688
Einzelheiten zur Richtlinie 2688
Version der Richtlinie 2688
JSON-Richtliniendokument 2688
Weitere Informationen 2689
AWSLambdaENIManagementAccess 2689
Diese Richtlinie wird verwendet 2689
Einzelheiten zur Richtlinie 2689
Version der Richtlinie 2689
JSON-Richtliniendokument 2690
Weitere Informationen 2690
AWSLambdaExecute 2690
Diese Richtlinie wird verwendet 2690
Einzelheiten zur Richtlinie 2691
Version der Richtlinie 2691
JSON-Richtliniendokument 2691
Weitere Informationen 2692

AWSLambdaFullAccess 2692
Diese Richtlinie wird verwendet 2692
Einzelheiten zur Richtlinie 2692
Version der Richtlinie 2692
JSON-Richtliniendokument 2693
Weitere Informationen 2694
AWSLambdaInvocation-DynamoDB 2694
Diese Richtlinie wird verwendet 2694
Einzelheiten zur Richtlinie 2695
Version der Richtlinie 2695
JSON-Richtliniendokument 2695
Weitere Informationen 2696
AWSLambdaKinesisExecutionRole 2696
Diese Richtlinie wird verwendet 2696
Einzelheiten zur Richtlinie 2696
Version der Richtlinie 2696
JSON-Richtliniendokument 2697
Weitere Informationen 2697
AWSLambdaManagedEC2ResourceOperator 2697
Diese Richtlinie wird verwendet 2698
Einzelheiten zur Richtlinie 2698
Version der Richtlinie 2698
JSON-Richtliniendokument 2698
Weitere Informationen 2700
AWSLambdaMSKExecutionRole 2700
Diese Richtlinie wird verwendet 2700
Einzelheiten zur Richtlinie 2700
Version der Richtlinie 2700
JSON-Richtliniendokument 2701
Weitere Informationen 2701
AWSLambdaReplicator 2701
Diese Richtlinie wird verwendet 2702
Einzelheiten der Richtlinie 2702
Version der Richtlinie 2702
JSON-Richtliniendokument 2702
Weitere Informationen 2703

AWSLambdaRole 2703
Diese Richtlinie wird verwendet 2704
Einzelheiten zur Richtlinie 2704
Version der Richtlinie 2704
JSON-Richtliniendokument 2704
Weitere Informationen 2705
AWSLambdaServiceRolePolicy 2705
Diese Richtlinie wird verwendet 2705
Einzelheiten der Richtlinie 2705
Version der Richtlinie 2705
JSON-Richtliniendokument 2706
Weitere Informationen 2706
AWSLambdaSQSQueueExecutionRole 2707
Diese Richtlinie wird verwendet 2707
Einzelheiten zur Richtlinie 2707
Version der Richtlinie 2707
JSON-Richtliniendokument 2707
Weitere Informationen 2708
AWSLambdaVPCAccessExecutionRole 2708
Diese Richtlinie wird verwendet 2708
Einzelheiten zur Richtlinie 2708
Version der Richtlinie 2709
JSON-Richtliniendokument 2709
Weitere Informationen 2709
AWSLicenseManagerConsumptionPolicy 2710
Diese Richtlinie wird verwendet 2710
Einzelheiten zur Richtlinie 2710
Version der Richtlinie 2710
JSON-Richtliniendokument 2710
Weitere Informationen 2711
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 2711
Diese Richtlinie wird verwendet 2711
Einzelheiten der Richtlinie 2711
Version der Richtlinie 2712
JSON-Richtliniendokument 2712
Weitere Informationen 2713

AWSLicenseManagerMasterAccountRolePolicy 2714
Diese Richtlinie wird verwendet 2714
Einzelheiten der Richtlinie 2714
Version der Richtlinie 2714
JSON-Richtliniendokument 2714
Weitere Informationen 2719
AWSLicenseManagerMemberAccountRolePolicy 2719
Diese Richtlinie wird verwendet 2720
Einzelheiten der Richtlinie 2720
Version der Richtlinie 2720
JSON-Richtliniendokument 2720
Weitere Informationen 2721
AWSLicenseManagerServiceRolePolicy 2721
Diese Richtlinie wird verwendet 2722
Einzelheiten der Richtlinie 2722
Version der Richtlinie 2722
JSON-Richtliniendokument 2722
Weitere Informationen 2726
AWSLicenseManagerUserSubscriptionsServiceRolePolicy 2726
Diese Richtlinie wird verwendet 2726
Einzelheiten der Richtlinie 2726
Version der Richtlinie 2726
JSON-Richtliniendokument 2727
Weitere Informationen 2730
AWSM2ServicePolicy 2730
Diese Richtlinie wird verwendet 2730
Einzelheiten der Richtlinie 2730
Version der Richtlinie 2730
JSON-Richtliniendokument 2731
Weitere Informationen 2732
AWSManagedServices_ContactsServiceRolePolicy 2732
Diese Richtlinie wird verwendet 2732
Einzelheiten der Richtlinie 2732
Version der Richtlinie 2733
JSON-Richtliniendokument 2733
Weitere Informationen 2734

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy 2734
Diese Richtlinie wird verwendet 2734
Einzelheiten der Richtlinie 2734
Version der Richtlinie 2734
JSON-Richtliniendokument 2735
Weitere Informationen 2736
AWSManagedServices_EventsServiceRolePolicy 2736
Diese Richtlinie wird verwendet 2736
Einzelheiten der Richtlinie 2737
Version der Richtlinie 2737
JSON-Richtliniendokument 2737
Weitere Informationen 2738
AWSManagedServices_SelfServiceReporting_ServiceRolePolicy 2738
Diese Richtlinie wird verwendet 2738
Einzelheiten der Richtlinie 2738
Version der Richtlinie 2739
JSON-Richtliniendokument 2739
Weitere Informationen 2739
AWSManagedServicesDeploymentToolkitPolicy 2739
Diese Richtlinie wird verwendet 2740
Einzelheiten der Richtlinie 2740
Version der Richtlinie 2740
JSON-Richtliniendokument 2740
Weitere Informationen 2742
AWSManagementConsoleAdministratorAccess 2742
Diese Richtlinie wird verwendet 2743
Einzelheiten zur Richtlinie 2743
Version der Richtlinie 2743
JSON-Richtliniendokument 2743
Weitere Informationen 2745
AWSManagementConsoleBasicUserAccess 2746
Diese Richtlinie wird verwendet 2746
Einzelheiten zur Richtlinie 2746
Version der Richtlinie 2746
JSON-Richtliniendokument 2746
Weitere Informationen 2747

AWSMarketplaceAmiIngestion 2748
Diese Richtlinie wird verwendet 2748
Einzelheiten zur Richtlinie 2748
Version der Richtlinie 2748
JSON-Richtliniendokument 2748
Weitere Informationen 2749
AWSMarketplaceDeploymentServiceRolePolicy 2749
Diese Richtlinie wird verwendet 2749
Einzelheiten der Richtlinie 2749
Version der Richtlinie 2750
JSON-Richtliniendokument 2750
Weitere Informationen 2751
AWSMarketplaceFullAccess 2751
Diese Richtlinie wird verwendet 2752
Einzelheiten zur Richtlinie 2752
Version der Richtlinie 2752
JSON-Richtliniendokument 2752
Weitere Informationen 2754
AWSMarketplaceGetEntitlements 2754
Diese Richtlinie wird verwendet 2754
Einzelheiten zur Richtlinie 2754
Version der Richtlinie 2755
JSON-Richtliniendokument 2755
Weitere Informationen 2755
AWSMarketplaceImageBuildFullAccess 2755
Diese Richtlinie wird verwendet 2756
Einzelheiten zur Richtlinie 2756
Version der Richtlinie 2756
JSON-Richtliniendokument 2756
Weitere Informationen 2760
AWSMarketplaceLicenseManagementServiceRolePolicy 2760
Diese Richtlinie wird verwendet 2760
Einzelheiten der Richtlinie 2760
Version der Richtlinie 2760
JSON-Richtliniendokument 2761
Weitere Informationen 2761

AWSMarketplaceManageSubscriptions 2761
Diese Richtlinie wird verwendet 2762
Einzelheiten zur Richtlinie 2762
Version der Richtlinie 2762
JSON-Richtliniendokument 2762
Weitere Informationen 2764
AWSMarketplaceMeteringFullAccess 2765
Diese Richtlinie wird verwendet 2765
Einzelheiten zur Richtlinie 2765
Version der Richtlinie 2765
JSON-Richtliniendokument 2765
Weitere Informationen 2766
AWSMarketplaceMeteringRegisterUsage 2766
Diese Richtlinie wird verwendet 2766
Einzelheiten zur Richtlinie 2766
Version der Richtlinie 2766
JSON-Richtliniendokument 2767
Weitere Informationen 2767
AWSMarketplaceProcurementSystemAdminFullAccess 2767
Diese Richtlinie wird verwendet 2767
Einzelheiten zur Richtlinie 2767
Version der Richtlinie 2768
JSON-Richtliniendokument 2768
Weitere Informationen 2768
AWSMarketplacePurchaseOrdersServiceRolePolicy 2769
Diese Richtlinie wird verwendet 2769
Einzelheiten der Richtlinie 2769
Version der Richtlinie 2769
JSON-Richtliniendokument 2769
Weitere Informationen 2770
AWSMarketplaceRead-only 2770
Diese Richtlinie wird verwendet 2770
Einzelheiten zur Richtlinie 2770
Version der Richtlinie 2770
JSON-Richtliniendokument 2771
Weitere Informationen 2772

AWSMarketplaceResaleAuthorizationServiceRolePolicy 2772
Diese Richtlinie wird verwendet 2772
Einzelheiten der Richtlinie 2772
Version der Richtlinie 2773
JSON-Richtliniendokument 2773
Weitere Informationen 2775
AWSMarketplaceSellerFullAccess 2775
Diese Richtlinie wird verwendet 2776
Einzelheiten zur Richtlinie 2776
Version der Richtlinie 2776
JSON-Richtliniendokument 2776
Weitere Informationen 2780
AWSMarketplaceSellerOfferManagement 2780
Diese Richtlinie wird verwendet 2780
Einzelheiten zur Richtlinie 2780
Version der Richtlinie 2781
JSON-Richtliniendokument 2781
Weitere Informationen 2783
AWSMarketplaceSellerProductsFullAccess 2783
Diese Richtlinie wird verwendet 2783
Einzelheiten zur Richtlinie 2783
Version der Richtlinie 2784
JSON-Richtliniendokument 2784
Weitere Informationen 2787
AWSMarketplaceSellerProductsReadOnly 2787
Diese Richtlinie wird verwendet 2787
Einzelheiten zur Richtlinie 2787
Version der Richtlinie 2787
JSON-Richtliniendokument 2788
Weitere Informationen 2789
AWSMcpServiceActionsFullAccess 2789
Diese Richtlinie wird verwendet 2789
Einzelheiten zur Richtlinie 2789
Version der Richtlinie 2789
JSON-Richtliniendokument 2790
Weitere Informationen 2790

AWSMediaConnectServicePolicy 2790
Diese Richtlinie wird verwendet 2790
Einzelheiten der Richtlinie 2791
Version der Richtlinie 2791
JSON-Richtliniendokument 2791
Weitere Informationen 2793
AWSMediaLiveAnywhereServiceRolePolicy 2793
Diese Richtlinie wird verwendet 2793
Einzelheiten der Richtlinie 2793
Version der Richtlinie 2794
JSON-Richtliniendokument 2794
Weitere Informationen 2797
AWSMediaTailorServiceRolePolicy 2797
Diese Richtlinie wird verwendet 2797
Einzelheiten der Richtlinie 2797
Version der Richtlinie 2797
JSON-Richtliniendokument 2798
Weitere Informationen 2798
AWSMigrationHubDiscoveryAccess 2798
Diese Richtlinie wird verwendet 2799
Einzelheiten zur Richtlinie 2799
Version der Richtlinie 2799
JSON-Richtliniendokument 2799
Weitere Informationen 2800
AWSMigrationHubDMSAccess 2801
Diese Richtlinie wird verwendet 2801
Einzelheiten zur Richtlinie 2801
Version der Richtlinie 2801
JSON-Richtliniendokument 2801
Weitere Informationen 2802
AWSMigrationHubFullAccess 2802
Diese Richtlinie wird verwendet 2803
Einzelheiten zur Richtlinie 2803
Version der Richtlinie 2803
JSON-Richtliniendokument 2803
Weitere Informationen 2805

AWSMigrationHubOrchestratorConsoleFullAccess ... 2805
Diese Richtlinie wird verwendet ... 2805
Einzelheiten zur Richtlinie ... 2805
Version der Richtlinie ... 2805
JSON-Richtliniendokument ... 2806
Weitere Informationen ... 2809
AWSMigrationHubOrchestratorInstanceRolePolicy ... 2809
Diese Richtlinie wird verwendet ... 2809
Einzelheiten zur Richtlinie ... 2809
Version der Richtlinie ... 2809
JSON-Richtliniendokument ... 2810
Weitere Informationen ... 2810
AWSMigrationHubOrchestratorPlugin ... 2810
Diese Richtlinie wird verwendet ... 2811
Einzelheiten zur Richtlinie ... 2811
Version der Richtlinie ... 2811
JSON-Richtliniendokument ... 2811
Weitere Informationen ... 2812
AWSMigrationHubOrchestratorServiceRolePolicy ... 2813
Diese Richtlinie wird verwendet ... 2813
Einzelheiten der Richtlinie ... 2813
Version der Richtlinie ... 2813
JSON-Richtliniendokument ... 2813
Weitere Informationen ... 2817
AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess ... 2817
Diese Richtlinie wird verwendet ... 2817
Einzelheiten zur Richtlinie ... 2817
Version der Richtlinie ... 2818
JSON-Richtliniendokument ... 2818
Weitere Informationen ... 2823
AWSMigrationHubRefactorSpaces-SSMAutomationPolicy ... 2824
Diese Richtlinie wird verwendet ... 2824
Einzelheiten zur Richtlinie ... 2824
Version der Richtlinie ... 2824
JSON-Richtliniendokument ... 2824
Weitere Informationen ... 2826

AWSMigrationHubRefactorSpacesFullAccess 2826
Diese Richtlinie wird verwendet 2826
Einzelheiten zur Richtlinie 2826
Version der Richtlinie 2827
JSON-Richtliniendokument 2827
Weitere Informationen 2833
AWSMigrationHubRefactorSpacesServiceRolePolicy 2833
Diese Richtlinie wird verwendet 2834
Einzelheiten der Richtlinie 2834
Version der Richtlinie 2834
JSON-Richtliniendokument 2834
Weitere Informationen 2838
AWSMigrationHubSMSAccess 2838
Diese Richtlinie wird verwendet 2838
Einzelheiten zur Richtlinie 2838
Version der Richtlinie 2839
JSON-Richtliniendokument 2839
Weitere Informationen 2840
AWSMigrationHubStrategyCollector 2840
Diese Richtlinie wird verwendet 2840
Einzelheiten zur Richtlinie 2840
Version der Richtlinie 2841
JSON-Richtliniendokument 2841
Weitere Informationen 2843
AWSMigrationHubStrategyConsoleFullAccess 2843
Diese Richtlinie wird verwendet 2843
Einzelheiten zur Richtlinie 2844
Version der Richtlinie 2844
JSON-Richtliniendokument 2844
Weitere Informationen 2846
AWSMigrationHubStrategyServiceRolePolicy 2846
Diese Richtlinie wird verwendet 2846
Einzelheiten der Richtlinie 2846
Version der Richtlinie 2846
JSON-Richtliniendokument 2847
Weitere Informationen 2848

AWSMobileHub_FullAccess 2848
Diese Richtlinie wird verwendet 2848
Einzelheiten zur Richtlinie 2848
Version der Richtlinie 2848
JSON-Richtliniendokument 2849
Weitere Informationen 2850
AWSMobileHub_ReadOnly 2850
Diese Richtlinie wird verwendet 2850
Einzelheiten zur Richtlinie 2851
Version der Richtlinie 2851
JSON-Richtliniendokument 2851
Weitere Informationen 2852
AWSMSKReplicatorExecutionRole 2852
Diese Richtlinie wird verwendet 2853
Einzelheiten zur Richtlinie 2853
Version der Richtlinie 2853
JSON-Richtliniendokument 2853
Weitere Informationen 2854
AWSNATGatewayServiceRolePolicy 2855
Diese Richtlinie wird verwendet 2855
Einzelheiten der Richtlinie 2855
Version der Richtlinie 2855
JSON-Richtliniendokument 2855
Weitere Informationen 2856
AWSNetworkFirewallFullAccess 2856
Diese Richtlinie wird verwendet 2856
Einzelheiten zur Richtlinie 2856
Version der Richtlinie 2857
JSON-Richtliniendokument 2857
Weitere Informationen 2861
AWSNetworkFirewallReadOnlyAccess 2861
Diese Richtlinie wird verwendet 2861
Einzelheiten zur Richtlinie 2861
Version der Richtlinie 2862
JSON-Richtliniendokument 2862
Weitere Informationen 2863

AWSNetworkFirewallServiceRolePolicy 2863
Diese Richtlinie wird verwendet 2863
Einzelheiten der Richtlinie 2863
Version der Richtlinie 2863
JSON-Richtliniendokument 2864
Weitere Informationen 2865
AWSNetworkManagerCloudWANServiceRolePolicy 2865
Diese Richtlinie wird verwendet 2866
Einzelheiten der Richtlinie 2866
Version der Richtlinie 2866
JSON-Richtliniendokument 2866
Weitere Informationen 2867
AWSNetworkManagerFullAccess 2867
Diese Richtlinie wird verwendet 2867
Einzelheiten zur Richtlinie 2867
Version der Richtlinie 2867
JSON-Richtliniendokument 2867
Weitere Informationen 2868
AWSNetworkManagerReadOnlyAccess 2868
Diese Richtlinie wird verwendet 2869
Einzelheiten zur Richtlinie 2869
Version der Richtlinie 2869
JSON-Richtliniendokument 2869
Weitere Informationen 2870
AWSNetworkManagerServiceRolePolicy 2870
Diese Richtlinie wird verwendet 2870
Einzelheiten der Richtlinie 2870
Version der Richtlinie 2870
JSON-Richtliniendokument 2871
Weitere Informationen 2872
AWSObservabilityAdminLogsCentralizationServiceRolePolicy 2872
Diese Richtlinie wird verwendet 2872
Einzelheiten der Richtlinie 2872
Version der Richtlinie 2872
JSON-Richtliniendokument 2873
Weitere Informationen 2873

AWSObservabilityAdminServiceRolePolicy 2874
Diese Richtlinie wird verwendet 2874
Einzelheiten der Richtlinie 2874
Version der Richtlinie 2874
JSON-Richtliniendokument 2874
Weitere Informationen 2877
AWSObservabilityAdminTelemetryEnablementServiceRolePolicy 2877
Diese Richtlinie wird verwendet 2877
Einzelheiten der Richtlinie 2877
Version der Richtlinie 2878
JSON-Richtliniendokument 2878
Weitere Informationen 2888
AWSOrganizationsFullAccess 2888
Diese Richtlinie wird verwendet 2888
Einzelheiten zur Richtlinie 2888
Version der Richtlinie 2888
JSON-Richtliniendokument 2889
Weitere Informationen 2890
AWSOrganizationsReadOnlyAccess 2890
Diese Richtlinie wird verwendet 2890
Einzelheiten zur Richtlinie 2890
Version der Richtlinie 2890
JSON-Richtliniendokument 2891
Weitere Informationen 2891
AWSOrganizationsServiceTrustPolicy 2892
Diese Richtlinie wird verwendet 2892
Einzelheiten der Richtlinie 2892
Version der Richtlinie 2892
JSON-Richtliniendokument 2892
Weitere Informationen 2893
AWSOutpostsAuthorizeServerPolicy 2893
Diese Richtlinie wird verwendet 2893
Einzelheiten zur Richtlinie 2893
Version der Richtlinie 2894
JSON-Richtliniendokument 2894
Weitere Informationen 2894

AWSOutpostsServiceRolePolicy 2895
Diese Richtlinie wird verwendet 2895
Einzelheiten der Richtlinie 2895
Version der Richtlinie 2895
JSON-Richtliniendokument 2895
Weitere Informationen 2897
AWSPanoramaApplianceRolePolicy 2897
Diese Richtlinie wird verwendet 2897
Einzelheiten zur Richtlinie 2898
Version der Richtlinie 2898
JSON-Richtliniendokument 2898
Weitere Informationen 2899
AWSPanoramaApplianceServiceRolePolicy 2899
Diese Richtlinie wird verwendet 2899
Einzelheiten zur Richtlinie 2899
Version der Richtlinie 2899
JSON-Richtliniendokument 2900
Weitere Informationen 2901
AWSPanoramaFullAccess 2901
Diese Richtlinie wird verwendet 2901
Einzelheiten zur Richtlinie 2902
Version der Richtlinie 2902
JSON-Richtliniendokument 2902
Weitere Informationen 2904
AWSPanoramaGreengrassGroupRolePolicy 2905
Diese Richtlinie wird verwendet 2905
Einzelheiten zur Richtlinie 2905
Version der Richtlinie 2905
JSON-Richtliniendokument 2905
Weitere Informationen 2907
AWSPanoramaSageMakerRolePolicy 2907
Diese Richtlinie wird verwendet 2907
Einzelheiten zur Richtlinie 2907
Version der Richtlinie 2907
JSON-Richtliniendokument 2908
Weitere Informationen 2908

AWSPanoramaServiceLinkedRolePolicy 2908
Diese Richtlinie wird verwendet 2909
Einzelheiten der Richtlinie 2909
Version der Richtlinie 2909
JSON-Richtliniendokument 2909
Weitere Informationen 2912
AWSPanoramaServiceRolePolicy 2912
Diese Richtlinie wird verwendet 2912
Einzelheiten zur Richtlinie 2912
Version der Richtlinie 2912
JSON-Richtliniendokument 2913
Weitere Informationen 2920
AWSPartnerCentralChannelHandshakeApprovalManagement 2920
Diese Richtlinie wird verwendet 2920
Einzelheiten zur Richtlinie 2920
Version der Richtlinie 2920
JSON-Richtliniendokument 2921
Weitere Informationen 2921
AWSPartnerCentralChannelManagement 2921
Diese Richtlinie wird verwendet 2922
Einzelheiten zur Richtlinie 2922
Version der Richtlinie 2922
JSON-Richtliniendokument 2922
Weitere Informationen 2925
AWSPartnerCentralFullAccess 2925
Diese Richtlinie wird verwendet 2925
Einzelheiten zur Richtlinie 2925
Version der Richtlinie 2925
JSON-Richtliniendokument 2926
Weitere Informationen 2929
AWSPartnerCentralMarketingManagement 2929
Diese Richtlinie wird verwendet 2929
Einzelheiten zur Richtlinie 2929
Version der Richtlinie 2930
JSON-Richtliniendokument 2930
Weitere Informationen 2932

AWSPartnerCentralOpportunityManagement 2932
Diese Richtlinie wird verwendet 2932
Einzelheiten zur Richtlinie 2932
Version der Richtlinie 2933
JSON-Richtliniendokument 2933
Weitere Informationen 2936
AWSPartnerCentralSandboxFullAccess 2937
Diese Richtlinie wird verwendet 2937
Einzelheiten zur Richtlinie 2937
Version der Richtlinie 2937
JSON-Richtliniendokument 2937
Weitere Informationen 2938
AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy 2939
Diese Richtlinie wird verwendet 2939
Einzelheiten zur Richtlinie 2939
Version der Richtlinie 2939
JSON-Richtliniendokument 2939
Weitere Informationen 2940
AWSPartnerLedSupportReadOnlyAccess 2940
Diese Richtlinie wird verwendet 2940
Einzelheiten zur Richtlinie 2941
Version der Richtlinie 2941
JSON-Richtliniendokument 2941
Weitere Informationen 2978
AWSPCSComputeNodePolicy 2978
Diese Richtlinie wird verwendet 2978
Einzelheiten zur Richtlinie 2978
Version der Richtlinie 2979
JSON-Richtliniendokument 2979
Weitere Informationen 2979
AWSPCSServiceRolePolicy 2979
Diese Richtlinie wird verwendet 2980
Einzelheiten der Richtlinie 2980
Version der Richtlinie 2980
JSON-Richtliniendokument 2980
Weitere Informationen 2985

AWSPriceListServiceFullAccess 2985
Diese Richtlinie wird verwendet 2985
Einzelheiten zur Richtlinie 2985
Version der Richtlinie 2986
JSON-Richtliniendokument 2986
Weitere Informationen 2986
AWSPrivateCAAuditor 2987
Diese Richtlinie wird verwendet 2987
Einzelheiten zur Richtlinie 2987
Version der Richtlinie 2987
JSON-Richtliniendokument 2987
Weitere Informationen 2988
AWSPrivateCAConnectorForKubernetesPolicy 2988
Diese Richtlinie wird verwendet 2988
Einzelheiten zur Richtlinie 2988
Version der Richtlinie 2989
JSON-Richtliniendokument 2989
Weitere Informationen 2989
AWSPrivateCAFullAccess 2990
Diese Richtlinie wird verwendet 2990
Einzelheiten zur Richtlinie 2990
Version der Richtlinie 2990
JSON-Richtliniendokument 2990
Weitere Informationen 2991
AWSPrivateCAPrivilegedUser 2991
Diese Richtlinie wird verwendet 2991
Einzelheiten zur Richtlinie 2991
Version der Richtlinie 2991
JSON-Richtliniendokument 2992
Weitere Informationen 2993
AWSPrivateCAReadOnly 2993
Diese Richtlinie wird verwendet 2993
Einzelheiten zur Richtlinie 2993
Version der Richtlinie 2993
JSON-Richtliniendokument 2994
Weitere Informationen 2994

AWSPrivateCAUser 2994
Diese Richtlinie wird verwendet 2995
Einzelheiten zur Richtlinie 2995
Version der Richtlinie 2995
JSON-Richtliniendokument 2995
Weitere Informationen 2996
AWSPrivateMarketplaceAdminFullAccess 2997
Diese Richtlinie wird verwendet 2997
Einzelheiten zur Richtlinie 2997
Version der Richtlinie 2997
JSON-Richtliniendokument 2997
Weitere Informationen 3000
AWSPrivateMarketplaceRequests 3000
Diese Richtlinie wird verwendet 3000
Einzelheiten zur Richtlinie 3000
Version der Richtlinie 3001
JSON-Richtliniendokument 3001
Weitere Informationen 3003
AWSPrivateNetworksServiceRolePolicy 3003
Diese Richtlinie wird verwendet 3003
Einzelheiten der Richtlinie 3003
Version der Richtlinie 3004
JSON-Richtliniendokument 3004
Weitere Informationen 3004
AWSProtonCodeBuildProvisioningBasicAccess 3004
Diese Richtlinie wird verwendet 3005
Einzelheiten zur Richtlinie 3005
Version der Richtlinie 3005
JSON-Richtliniendokument 3005
Weitere Informationen 3006
AWSProtonCodeBuildProvisioningServiceRolePolicy 3006
Diese Richtlinie wird verwendet 3006
Einzelheiten der Richtlinie 3006
Version der Richtlinie 3007
JSON-Richtliniendokument 3007
Weitere Informationen 3008

AWSProtonDeveloperAccess 3008
Diese Richtlinie wird verwendet 3008
Einzelheiten zur Richtlinie 3008
Version der Richtlinie 3009
JSON-Richtliniendokument 3009
Weitere Informationen 3011
AWSProtonFullAccess 3011
Diese Richtlinie wird verwendet 3012
Einzelheiten zur Richtlinie 3012
Version der Richtlinie 3012
JSON-Richtliniendokument 3012
Weitere Informationen 3014
AWSProtonReadOnlyAccess 3015
Diese Richtlinie wird verwendet 3015
Einzelheiten zur Richtlinie 3015
Version der Richtlinie 3015
JSON-Richtliniendokument 3015
Weitere Informationen 3017
AWSProtonServiceGitSyncServiceRolePolicy 3017
Diese Richtlinie wird verwendet 3017
Einzelheiten der Richtlinie 3017
Version der Richtlinie 3017
JSON-Richtliniendokument 3018
Weitere Informationen 3018
AWSProtonSyncServiceRolePolicy 3019
Diese Richtlinie wird verwendet 3019
Einzelheiten der Richtlinie 3019
Version der Richtlinie 3019
JSON-Richtliniendokument 3019
Weitere Informationen 3020
AWSPurchaseOrdersServiceRolePolicy 3021
Diese Richtlinie wird verwendet 3021
Einzelheiten zur Richtlinie 3021
Version der Richtlinie 3021
JSON-Richtliniendokument 3021
Weitere Informationen 3022

AWSQuickSetupCFGCPacksPermissionsBoundary 3022
Diese Richtlinie wird verwendet 3023
Einzelheiten zur Richtlinie 3023
Version der Richtlinie 3023
JSON-Richtliniendokument 3023
Weitere Informationen 3026
AWSQuickSetupDeploymentRolePolicy 3026
Diese Richtlinie wird verwendet 3026
Einzelheiten zur Richtlinie 3026
Version der Richtlinie 3027
JSON-Richtliniendokument 3027
Weitere Informationen 3035
AWSQuickSetupDevOpsGuruPermissionsBoundary 3035
Diese Richtlinie wird verwendet 3036
Einzelheiten zur Richtlinie 3036
Version der Richtlinie 3036
JSON-Richtliniendokument 3036
Weitere Informationen 3039
AWSQuickSetupDistributorPermissionsBoundary 3039
Diese Richtlinie wird verwendet 3039
Einzelheiten zur Richtlinie 3039
Version der Richtlinie 3040
JSON-Richtliniendokument 3040
Weitere Informationen 3045
AWSQuickSetupEnableAREXExecutionPolicy 3046
Diese Richtlinie wird verwendet 3046
Einzelheiten zur Richtlinie 3046
Version der Richtlinie 3046
JSON-Richtliniendokument 3046
Weitere Informationen 3048
AWSQuickSetupEnableDHMCExecutionPolicy 3048
Diese Richtlinie wird verwendet 3048
Einzelheiten zur Richtlinie 3049
Version der Richtlinie 3049
JSON-Richtliniendokument 3049
Weitere Informationen 3050

AWSQuickSetupJITNADeploymentRolePolicy 3050
Diese Richtlinie wird verwendet 3051
Einzelheiten zur Richtlinie 3051
Version der Richtlinie 3051
JSON-Richtliniendokument 3051
Weitere Informationen 3055
AWSQuickSetupManagedInstanceProfileExecutionPolicy 3055
Diese Richtlinie wird verwendet 3055
Einzelheiten zur Richtlinie 3055
Version der Richtlinie 3055
JSON-Richtliniendokument 3056
Weitere Informationen 3060
AWSQuickSetupManageJITNAResourcesExecutionPolicy 3060
Diese Richtlinie wird verwendet 3060
Einzelheiten zur Richtlinie 3060
Version der Richtlinie 3061
JSON-Richtliniendokument 3061
Weitere Informationen 3063
AWSQuickSetupPatchPolicyBaselineAccess 3063
Diese Richtlinie wird verwendet 3063
Einzelheiten zur Richtlinie 3063
Version der Richtlinie 3064
JSON-Richtliniendokument 3064
Weitere Informationen 3065
AWSQuickSetupPatchPolicyDeploymentRolePolicy 3065
Diese Richtlinie wird verwendet 3065
Einzelheiten zur Richtlinie 3065
Version der Richtlinie 3065
JSON-Richtliniendokument 3066
Weitere Informationen 3073
AWSQuickSetupPatchPolicyPermissionsBoundary 3074
Diese Richtlinie wird verwendet 3074
Einzelheiten zur Richtlinie 3074
Version der Richtlinie 3074
JSON-Richtliniendokument 3074
Weitere Informationen 3083

AWSQuickSetupSchedulerPermissionsBoundary 3083
Diese Richtlinie wird verwendet 3083
Einzelheiten zur Richtlinie 3083
Version der Richtlinie 3083
JSON-Richtliniendokument 3084
Weitere Informationen 3087
AWSQuickSetupSSMDeploymentRolePolicy 3087
Diese Richtlinie wird verwendet 3087
Einzelheiten zur Richtlinie 3087
Version der Richtlinie 3088
JSON-Richtliniendokument 3088
Weitere Informationen 3098
AWSQuickSetupSSMDeploymentS3BucketRolePolicy 3099
Diese Richtlinie wird verwendet 3099
Einzelheiten zur Richtlinie 3099
Version der Richtlinie 3099
JSON-Richtliniendokument 3099
Weitere Informationen 3100
AWSQuickSetupSSMHostMgmtPermissionsBoundary 3100
Diese Richtlinie wird verwendet 3101
Einzelheiten zur Richtlinie 3101
Version der Richtlinie 3101
JSON-Richtliniendokument 3101
Weitere Informationen 3107
AWSQuickSetupSSMLifecycleManagementExecutionPolicy 3107
Diese Richtlinie wird verwendet 3107
Einzelheiten zur Richtlinie 3108
Version der Richtlinie 3108
JSON-Richtliniendokument 3108
Weitere Informationen 3109
AWSQuickSetupSSMManageResourcesExecutionPolicy 3110
Diese Richtlinie wird verwendet 3110
Einzelheiten zur Richtlinie 3110
Version der Richtlinie 3110
JSON-Richtliniendokument 3110
Weitere Informationen 3113

AWSQuickSetupStartSSMAssociationsExecutionPolicy 3113
Diese Richtlinie wird verwendet 3113
Einzelheiten zur Richtlinie 3114
Version der Richtlinie 3114
JSON-Richtliniendokument 3114
Weitere Informationen 3115
AWSQuickSetupStartStopInstancesExecutionPolicy 3115
Diese Richtlinie wird verwendet 3115
Einzelheiten zur Richtlinie 3116
Version der Richtlinie 3116
JSON-Richtliniendokument 3116
Weitere Informationen 3118
AWSQuickSightAssetBundleExportPolicy 3118
Diese Richtlinie wird verwendet 3118
Einzelheiten zur Richtlinie 3118
Version der Richtlinie 3118
JSON-Richtliniendokument 3119
Weitere Informationen 3121
AWSQuickSightAssetBundleImportPolicy 3121
Diese Richtlinie wird verwendet 3121
Einzelheiten zur Richtlinie 3121
Version der Richtlinie 3121
JSON-Richtliniendokument 3122
Weitere Informationen 3124
AWSQuicksightAthenaAccess 3125
Diese Richtlinie wird verwendet 3125
Einzelheiten zur Richtlinie 3125
Version der Richtlinie 3125
JSON-Richtliniendokument 3125
Weitere Informationen 3128
AWSQuickSightDescribeRDS 3128
Diese Richtlinie wird verwendet 3128
Einzelheiten zur Richtlinie 3128
Version der Richtlinie 3128
JSON-Richtliniendokument 3129
Weitere Informationen 3129

AWSQuickSightDescribeRedshift 3129
Diese Richtlinie wird verwendet 3129
Einzelheiten zur Richtlinie 3129
Version der Richtlinie 3130
JSON-Richtliniendokument 3130
Weitere Informationen 3130
AWSQuickSightElasticsearchPolicy 3130
Diese Richtlinie wird verwendet 3131
Einzelheiten zur Richtlinie 3131
Version der Richtlinie 3131
JSON-Richtliniendokument 3131
Weitere Informationen 3132
AWSQuickSightIoTAnalyticsAccess 3133
Diese Richtlinie wird verwendet 3133
Einzelheiten zur Richtlinie 3133
Version der Richtlinie 3133
JSON-Richtliniendokument 3133
Weitere Informationen 3134
AWSQuickSightListIAM 3134
Diese Richtlinie wird verwendet 3134
Einzelheiten zur Richtlinie 3134
Version der Richtlinie 3134
JSON-Richtliniendokument 3135
Weitere Informationen 3135
AWSQuicksightOpenSearchPolicy 3135
Diese Richtlinie wird verwendet 3135
Einzelheiten zur Richtlinie 3135
Version der Richtlinie 3136
JSON-Richtliniendokument 3136
Weitere Informationen 3137
AWSQuickSightSageMakerPolicy 3137
Diese Richtlinie wird verwendet 3137
Einzelheiten zur Richtlinie 3137
Version der Richtlinie 3138
JSON-Richtliniendokument 3138
Weitere Informationen 3139

AWSQuickSightSecretsManagerWriteAccess 3139
Diese Richtlinie wird verwendet 3140
Einzelheiten zur Richtlinie 3140
Version der Richtlinie 3140
JSON-Richtliniendokument 3140
Weitere Informationen 3141
AWSQuickSightSecretsManagerWritePolicy 3141
Diese Richtlinie wird verwendet 3141
Einzelheiten zur Richtlinie 3142
Version der Richtlinie 3142
JSON-Richtliniendokument 3142
Weitere Informationen 3143
AWSQuickSightTimestreamPolicy 3143
Diese Richtlinie wird verwendet 3143
Einzelheiten zur Richtlinie 3143
Version der Richtlinie 3144
JSON-Richtliniendokument 3144
Weitere Informationen 3144
AWSReachabilityAnalyzerServiceRolePolicy 3145
Diese Richtlinie wird verwendet 3145
Einzelheiten der Richtlinie 3145
Version der Richtlinie 3145
JSON-Richtliniendokument 3145
Weitere Informationen 3147
AWSRefactoringToolkitFullAccess 3148
Diese Richtlinie wird verwendet 3148
Einzelheiten zur Richtlinie 3148
Version der Richtlinie 3148
JSON-Richtliniendokument 3149
Weitere Informationen 3162
AWSRefactoringToolkitSidecarPolicy 3162
Diese Richtlinie wird verwendet 3163
Einzelheiten zur Richtlinie 3163
Version der Richtlinie 3163
JSON-Richtliniendokument 3163
Weitere Informationen 3164

AWSrePostPrivateCloudWatchAccess 3164
Diese Richtlinie wird verwendet 3164
Einzelheiten der Richtlinie 3165
Version der Richtlinie 3165
JSON-Richtliniendokument 3165
Weitere Informationen 3166
AWSRepostSpaceSupportOperationsPolicy 3166
Diese Richtlinie wird verwendet 3166
Einzelheiten zur Richtlinie 3166
Version der Richtlinie 3166
JSON-Richtliniendokument 3167
Weitere Informationen 3167
AWSResilienceHubAsssessmentExecutionPolicy 3167
Diese Richtlinie wird verwendet 3168
Einzelheiten zur Richtlinie 3168
Version der Richtlinie 3168
JSON-Richtliniendokument 3168
Weitere Informationen 3173
AWSResourceAccessManagerFullAccess 3173
Diese Richtlinie wird verwendet 3173
Einzelheiten zur Richtlinie 3173
Version der Richtlinie 3174
JSON-Richtliniendokument 3174
Weitere Informationen 3174
AWSResourceAccessManagerReadOnlyAccess 3174
Diese Richtlinie wird verwendet 3175
Einzelheiten zur Richtlinie 3175
Version der Richtlinie 3175
JSON-Richtliniendokument 3175
Weitere Informationen 3176
AWSResourceAccessManagerResourceShareParticipantAccess 3176
Diese Richtlinie wird verwendet 3176
Einzelheiten zur Richtlinie 3176
Version der Richtlinie 3176
JSON-Richtliniendokument 3177
Weitere Informationen 3177

AWSResourceAccessManagerServiceRolePolicy 3177
Diese Richtlinie wird verwendet 3178
Einzelheiten der Richtlinie 3178
Version der Richtlinie 3178
JSON-Richtliniendokument 3178
Weitere Informationen 3179
AWSResourceExplorerFullAccess 3179
Diese Richtlinie wird verwendet 3179
Einzelheiten zur Richtlinie 3179
Version der Richtlinie 3180
JSON-Richtliniendokument 3180
Weitere Informationen 3181
AWSResourceExplorerOrganizationsAccess 3181
Diese Richtlinie wird verwendet 3181
Einzelheiten zur Richtlinie 3181
Version der Richtlinie 3182
JSON-Richtliniendokument 3182
Weitere Informationen 3183
AWSResourceExplorerReadOnlyAccess 3184
Diese Richtlinie wird verwendet 3184
Einzelheiten zur Richtlinie 3184
Version der Richtlinie 3184
JSON-Richtliniendokument 3184
Weitere Informationen 3185
AWSResourceExplorerServiceRolePolicy 3185
Diese Richtlinie wird verwendet 3185
Einzelheiten der Richtlinie 3185
Version der Richtlinie 3186
JSON-Richtliniendokument 3186
Weitere Informationen 3205
AWSResourceGroupsReadOnlyAccess 3205
Diese Richtlinie wird verwendet 3205
Einzelheiten zur Richtlinie 3205
Version der Richtlinie 3205
JSON-Richtliniendokument 3206
Weitere Informationen 3207

AWSRoboMaker_FullAccess 3207
Diese Richtlinie wird verwendet 3207
Einzelheiten zur Richtlinie 3207
Version der Richtlinie 3208
JSON-Richtliniendokument 3208
Weitere Informationen 3209
AWSRoboMakerReadOnlyAccess 3209
Diese Richtlinie wird verwendet 3210
Einzelheiten zur Richtlinie 3210
Version der Richtlinie 3210
JSON-Richtliniendokument 3210
Weitere Informationen 3211
AWSRoboMakerServicePolicy 3211
Diese Richtlinie wird verwendet 3211
Einzelheiten der Richtlinie 3211
Version der Richtlinie 3211
JSON-Richtliniendokument 3212
Weitere Informationen 3213
AWSRoboMakerServiceRolePolicy 3213
Diese Richtlinie wird verwendet 3213
Einzelheiten zur Richtlinie 3214
Version der Richtlinie 3214
JSON-Richtliniendokument 3214
Weitere Informationen 3215
AWSRolesAnywhereFullAccess 3215
Diese Richtlinie wird verwendet 3216
Einzelheiten zur Richtlinie 3216
Version der Richtlinie 3216
JSON-Richtliniendokument 3216
Weitere Informationen 3218
AWSRolesAnywhereReadOnly 3219
Diese Richtlinie wird verwendet 3219
Einzelheiten zur Richtlinie 3219
Version der Richtlinie 3219
JSON-Richtliniendokument 3219
Weitere Informationen 3221

AWSRolesAnywhereServicePolicy 3221
Diese Richtlinie wird verwendet 3221
Einzelheiten der Richtlinie 3221
Version der Richtlinie 3222
JSON-Richtliniendokument 3222
Weitere Informationen 3223
AWSS3OnOutpostsServiceRolePolicy 3223
Diese Richtlinie wird verwendet 3223
Einzelheiten der Richtlinie 3223
Version der Richtlinie 3223
JSON-Richtliniendokument 3224
Weitere Informationen 3226
AWSSavingsPlansFullAccess 3226
Diese Richtlinie wird verwendet 3226
Einzelheiten zur Richtlinie 3227
Version der Richtlinie 3227
JSON-Richtliniendokument 3227
Weitere Informationen 3227
AWSSavingsPlansReadOnlyAccess 3228
Diese Richtlinie wird verwendet 3228
Einzelheiten zur Richtlinie 3228
Version der Richtlinie 3228
JSON-Richtliniendokument 3228
Weitere Informationen 3229
AWSSecretsManagerClientReadOnlyAccess 3229
Diese Richtlinie wird verwendet 3229
Einzelheiten zur Richtlinie 3229
Version der Richtlinie 3229
JSON-Richtliniendokument 3230
Weitere Informationen 3230
AWSSecurityHubFullAccess 3231
Diese Richtlinie wird verwendet 3231
Einzelheiten zur Richtlinie 3231
Version der Richtlinie 3231
JSON-Richtliniendokument 3231
Weitere Informationen 3233

AWSSecurityHubOrganizationsAccess 3233
Diese Richtlinie wird verwendet 3233
Einzelheiten zur Richtlinie 3233
Version der Richtlinie 3233
JSON-Richtliniendokument 3234
Weitere Informationen 3236
AWSSecurityHubReadOnlyAccess 3236
Diese Richtlinie wird verwendet 3236
Einzelheiten zur Richtlinie 3237
Version der Richtlinie 3237
JSON-Richtliniendokument 3237
Weitere Informationen 3237
AWSSecurityHubServiceRolePolicy 3238
Diese Richtlinie wird verwendet 3238
Einzelheiten der Richtlinie 3238
Version der Richtlinie 3238
JSON-Richtliniendokument 3238
Weitere Informationen 3240
AWSSecurityHubV2ServiceRolePolicy 3241
Diese Richtlinie wird verwendet 3241
Einzelheiten der Richtlinie 3241
Version der Richtlinie 3241
JSON-Richtliniendokument 3241
Weitere Informationen 3244
AWSSecurityIncidentResponseCaseFullAccess 3245
Diese Richtlinie wird verwendet 3245
Einzelheiten zur Richtlinie 3245
Version der Richtlinie 3245
JSON-Richtliniendokument 3245
Weitere Informationen 3247
AWSSecurityIncidentResponseFullAccess 3247
Diese Richtlinie wird verwendet 3247
Einzelheiten zur Richtlinie 3247
Version der Richtlinie 3247
JSON-Richtliniendokument 3248
Weitere Informationen 3250

AWSSecurityIncidentResponseReadOnlyAccess 3250
Diese Richtlinie wird verwendet 3250
Einzelheiten zur Richtlinie 3250
Version der Richtlinie 3251
JSON-Richtliniendokument 3251
Weitere Informationen 3251
AWSSecurityIncidentResponseServiceRolePolicy 3252
Diese Richtlinie wird verwendet 3252
Einzelheiten der Richtlinie 3252
Version der Richtlinie 3252
JSON-Richtliniendokument 3252
Weitere Informationen 3254
AWSSecurityIncidentResponseTriageServiceRolePolicy 3254
Diese Richtlinie wird verwendet 3254
Einzelheiten der Richtlinie 3254
Version der Richtlinie 3254
JSON-Richtliniendokument 3255
Weitere Informationen 3257
AWSServiceCatalogAdminFullAccess 3257
Diese Richtlinie wird verwendet 3257
Einzelheiten zur Richtlinie 3257
Version der Richtlinie 3258
JSON-Richtliniendokument 3258
Weitere Informationen 3261
AWSServiceCatalogAdminReadOnlyAccess 3261
Diese Richtlinie wird verwendet 3261
Einzelheiten zur Richtlinie 3261
Version der Richtlinie 3261
JSON-Richtliniendokument 3262
Weitere Informationen 3263
AWSServiceCatalogAppRegistryFullAccess 3263
Diese Richtlinie wird verwendet 3263
Einzelheiten zur Richtlinie 3263
Version der Richtlinie 3264
JSON-Richtliniendokument 3264
Weitere Informationen 3266

AWSServiceCatalogAppRegistryReadOnlyAccess 3266
Diese Richtlinie wird verwendet 3266
Einzelheiten zur Richtlinie 3266
Version der Richtlinie 3267
JSON-Richtliniendokument 3267
Weitere Informationen 3267
AWSServiceCatalogAppRegistryServiceRolePolicy 3268
Diese Richtlinie wird verwendet 3268
Einzelheiten der Richtlinie 3268
Version der Richtlinie 3268
JSON-Richtliniendokument 3268
Weitere Informationen 3270
AWSServiceCatalogEndUserFullAccess 3270
Diese Richtlinie wird verwendet 3270
Einzelheiten zur Richtlinie 3270
Version der Richtlinie 3270
JSON-Richtliniendokument 3271
Weitere Informationen 3273
AWSServiceCatalogEndUserReadOnlyAccess 3273
Diese Richtlinie wird verwendet 3273
Einzelheiten zur Richtlinie 3273
Version der Richtlinie 3273
JSON-Richtliniendokument 3274
Weitere Informationen 3275
AWSServiceCatalogOrgsDataSyncServiceRolePolicy 3275
Diese Richtlinie wird verwendet 3276
Einzelheiten der Richtlinie 3276
Version der Richtlinie 3276
JSON-Richtliniendokument 3276
Weitere Informationen 3277
AWSServiceCatalogSyncServiceRolePolicy 3277
Diese Richtlinie wird verwendet 3277
Einzelheiten der Richtlinie 3277
Version der Richtlinie 3278
JSON-Richtliniendokument 3278
Weitere Informationen 3279

AWSServiceRoleForAmazonEKSNodegroup ... 3279
Diese Richtlinie wird verwendet ... 3279
Einzelheiten der Richtlinie ... 3279
Version der Richtlinie ... 3280
JSON-Richtliniendokument ... 3280
Weitere Informationen ... 3285
AWSServiceRoleForAmazonQDeveloper ... 3286
Diese Richtlinie wird verwendet ... 3286
Einzelheiten der Richtlinie ... 3286
Version der Richtlinie ... 3286
JSON-Richtliniendokument ... 3286
Weitere Informationen ... 3287
AWSServiceRoleForAWSTransform ... 3287
Diese Richtlinie wird verwendet ... 3287
Einzelheiten der Richtlinie ... 3287
Version der Richtlinie ... 3288
JSON-Richtliniendokument ... 3288
Weitere Informationen ... 3290
AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy ... 3290
Diese Richtlinie wird verwendet ... 3290
Einzelheiten der Richtlinie ... 3291
Version der Richtlinie ... 3291
JSON-Richtliniendokument ... 3291
Weitere Informationen ... 3291
AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy ... 3292
Diese Richtlinie wird verwendet ... 3292
Einzelheiten der Richtlinie ... 3292
Version der Richtlinie ... 3292
JSON-Richtliniendokument ... 3292
Weitere Informationen ... 3293
AWSServiceRoleForCodeGuru-Profiler ... 3293
Diese Richtlinie wird verwendet ... 3293
Einzelheiten der Richtlinie ... 3293
Version der Richtlinie ... 3294
JSON-Richtliniendokument ... 3294
Weitere Informationen ... 3294

AWSServiceRoleForCodeWhispererPolicy 3294
Diese Richtlinie wird verwendet 3295
Einzelheiten der Richtlinie 3295
Version der Richtlinie 3295
JSON-Richtliniendokument 3295
Weitere Informationen 3297
AWSServiceRoleForEC2ScheduledInstances 3297
Diese Richtlinie wird verwendet 3297
Einzelheiten der Richtlinie 3297
Version der Richtlinie 3298
JSON-Richtliniendokument 3298
Weitere Informationen 3299
AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy 3299
Diese Richtlinie wird verwendet 3299
Einzelheiten der Richtlinie 3299
Version der Richtlinie 3299
JSON-Richtliniendokument 3300
Weitere Informationen 3300
AWSServiceRoleForImageBuilder 3300
Diese Richtlinie wird verwendet 3300
Einzelheiten der Richtlinie 3300
Version der Richtlinie 3301
JSON-Richtliniendokument 3301
Weitere Informationen 3311
AWSServiceRoleForIoTSiteWise 3312
Diese Richtlinie wird verwendet 3312
Einzelheiten der Richtlinie 3312
Version der Richtlinie 3312
JSON-Richtliniendokument 3312
Weitere Informationen 3314
AWSServiceRoleForLogDeliveryPolicy 3314
Diese Richtlinie wird verwendet 3314
Einzelheiten der Richtlinie 3314
Version der Richtlinie 3314
JSON-Richtliniendokument 3315
Weitere Informationen 3315

AWSServiceRoleForMonitronPolicy 3315
Diese Richtlinie wird verwendet 3316
Einzelheiten der Richtlinie 3316
Version der Richtlinie 3316
JSON-Richtliniendokument 3316
Weitere Informationen 3317
AWSServiceRoleForNeptuneGraphPolicy 3317
Diese Richtlinie wird verwendet 3317
Einzelheiten der Richtlinie 3317
Version der Richtlinie 3317
JSON-Richtliniendokument 3318
Weitere Informationen 3319
AWSServiceRoleForPrivateMarketplaceAdminPolicy 3319
Diese Richtlinie wird verwendet 3319
Einzelheiten der Richtlinie 3319
Version der Richtlinie 3320
JSON-Richtliniendokument 3320
Weitere Informationen 3322
AWSServiceRoleForProcurementInsightsPolicy 3322
Diese Richtlinie wird verwendet 3322
Einzelheiten der Richtlinie 3322
Version der Richtlinie 3322
JSON-Richtliniendokument 3323
Weitere Informationen 3323
AWSServiceRoleForSMS 3323
Diese Richtlinie wird verwendet 3323
Einzelheiten der Richtlinie 3324
Version der Richtlinie 3324
JSON-Richtliniendokument 3324
Weitere Informationen 3331
AWSServiceRoleForUserSubscriptions 3331
Diese Richtlinie wird verwendet 3331
Einzelheiten der Richtlinie 3331
Version der Richtlinie 3331
JSON-Richtliniendokument 3332
Weitere Informationen 3333

AWSServiceRolePolicyForBackupReports 3333
Diese Richtlinie wird verwendet 3333
Einzelheiten der Richtlinie 3334
Version der Richtlinie 3334
JSON-Richtliniendokument 3334
Weitere Informationen 3335
AWSServiceRolePolicyForBackupRestoreTesting 3335
Diese Richtlinie wird verwendet 3336
Einzelheiten der Richtlinie 3336
Version der Richtlinie 3336
JSON-Richtliniendokument 3336
Weitere Informationen 3339
AWSServiceRolePolicyForWorkspacesInstances 3339
Diese Richtlinie wird verwendet 3339
Einzelheiten der Richtlinie 3339
Version der Richtlinie 3340
JSON-Richtliniendokument 3340
Weitere Informationen 3341
AWSShieldDRTAccessPolicy 3341
Diese Richtlinie wird verwendet 3341
Einzelheiten zur Richtlinie 3341
Version der Richtlinie 3341
JSON-Richtliniendokument 3342
Weitere Informationen 3343
AWSShieldServiceRolePolicy 3343
Diese Richtlinie wird verwendet 3343
Einzelheiten der Richtlinie 3343
Version der Richtlinie 3343
JSON-Richtliniendokument 3344
Weitere Informationen 3344
AWSSocialMessagingServiceRolePolicy 3344
Diese Richtlinie wird verwendet 3344
Einzelheiten der Richtlinie 3345
Version der Richtlinie 3345
JSON-Richtliniendokument 3345
Weitere Informationen 3345

AWSSSMForSAPServiceLinkedRolePolicy 3346
Diese Richtlinie wird verwendet 3346
Einzelheiten der Richtlinie 3346
Version der Richtlinie 3346
JSON-Richtliniendokument 3346
Weitere Informationen 3355
AWSSSMOpsInsightsServiceRolePolicy 3355
Diese Richtlinie wird verwendet 3355
Einzelheiten der Richtlinie 3355
Version der Richtlinie 3356
JSON-Richtliniendokument 3356
Weitere Informationen 3357
AWSSSODirectoryAdministrator 3357
Diese Richtlinie wird verwendet 3357
Einzelheiten zur Richtlinie 3357
Version der Richtlinie 3357
JSON-Richtliniendokument 3357
Weitere Informationen 3358
AWSSSODirectoryReadOnly 3358
Diese Richtlinie wird verwendet 3359
Einzelheiten zur Richtlinie 3359
Version der Richtlinie 3359
JSON-Richtliniendokument 3359
Weitere Informationen 3360
AWSSSOMasterAccountAdministrator 3360
Diese Richtlinie wird verwendet 3360
Einzelheiten zur Richtlinie 3360
Version der Richtlinie 3361
JSON-Richtliniendokument 3361
Weitere Informationen 3364
AWSSSOMemberAccountAdministrator 3364
Diese Richtlinie wird verwendet 3364
Einzelheiten zur Richtlinie 3364
Version der Richtlinie 3365
JSON-Richtliniendokument 3365
Weitere Informationen 3367

AWSSSOReadOnly 3367
Diese Richtlinie wird verwendet 3367
Einzelheiten zur Richtlinie 3367
Version der Richtlinie 3368
JSON-Richtliniendokument 3368
Weitere Informationen 3369
AWSSSOServiceRolePolicy 3369
Diese Richtlinie wird verwendet 3370
Einzelheiten der Richtlinie 3370
Version der Richtlinie 3370
JSON-Richtliniendokument 3370
Weitere Informationen 3374
AWSStepFunctionsConsoleFullAccess 3374
Diese Richtlinie wird verwendet 3374
Einzelheiten zur Richtlinie 3374
Version der Richtlinie 3375
JSON-Richtliniendokument 3375
Weitere Informationen 3375
AWSStepFunctionsFullAccess 3376
Diese Richtlinie wird verwendet 3376
Einzelheiten zur Richtlinie 3376
Version der Richtlinie 3376
JSON-Richtliniendokument 3376
Weitere Informationen 3377
AWSStepFunctionsReadOnlyAccess 3377
Diese Richtlinie wird verwendet 3377
Einzelheiten zur Richtlinie 3377
Version der Richtlinie 3377
JSON-Richtliniendokument 3378
Weitere Informationen 3378
AWSStorageGatewayFullAccess 3379
Diese Richtlinie wird verwendet 3379
Einzelheiten zur Richtlinie 3379
Version der Richtlinie 3379
JSON-Richtliniendokument 3379
Weitere Informationen 3380

AWSStorageGatewayReadOnlyAccess 3380
Diese Richtlinie wird verwendet 3380
Einzelheiten zur Richtlinie 3381
Version der Richtlinie 3381
JSON-Richtliniendokument 3381
Weitere Informationen 3382
AWSStorageGatewayServiceRolePolicy 3382
Diese Richtlinie wird verwendet 3382
Einzelheiten der Richtlinie 3382
Version der Richtlinie 3382
JSON-Richtliniendokument 3383
Weitere Informationen 3383
AWSSupplyChainFederationAdminAccess 3383
Diese Richtlinie wird verwendet 3384
Einzelheiten zur Richtlinie 3384
Version der Richtlinie 3384
JSON-Richtliniendokument 3384
Weitere Informationen 3390
AWSSupportAccess 3390
Diese Richtlinie wird verwendet 3391
Einzelheiten zur Richtlinie 3391
Version der Richtlinie 3391
JSON-Richtliniendokument 3391
Weitere Informationen 3392
AWSSupportAppFullAccess 3392
Diese Richtlinie wird verwendet 3392
Einzelheiten zur Richtlinie 3392
Version der Richtlinie 3392
JSON-Richtliniendokument 3393
Weitere Informationen 3393
AWSSupportAppReadOnlyAccess 3394
Diese Richtlinie wird verwendet 3394
Einzelheiten zur Richtlinie 3394
Version der Richtlinie 3394
JSON-Richtliniendokument 3394
Weitere Informationen 3395

AWSSupportPlansFullAccess 3395
Diese Richtlinie wird verwendet 3395
Einzelheiten zur Richtlinie 3395
Version der Richtlinie 3395
JSON-Richtliniendokument 3396
Weitere Informationen 3396
AWSSupportPlansReadOnlyAccess 3396
Diese Richtlinie wird verwendet 3396
Einzelheiten zur Richtlinie 3397
Version der Richtlinie 3397
JSON-Richtliniendokument 3397
Weitere Informationen 3397
AWSSupportServiceRolePolicy 3398
Diese Richtlinie wird verwendet 3398
Einzelheiten der Richtlinie 3398
Version der Richtlinie 3398
JSON-Richtliniendokument 3398
Weitere Informationen 3491
AWSSystemsManagerAccountDiscoveryServicePolicy 3491
Diese Richtlinie wird verwendet 3491
Einzelheiten der Richtlinie 3491
Version der Richtlinie 3491
JSON-Richtliniendokument 3492
Weitere Informationen 3492
AWSSystemsManagerChangeManagementServicePolicy 3492
Diese Richtlinie wird verwendet 3493
Einzelheiten der Richtlinie 3493
Version der Richtlinie 3493
JSON-Richtliniendokument 3493
Weitere Informationen 3496
AWSSystemsManagerEnableConfigRecordingExecutionPolicy 3496
Diese Richtlinie wird verwendet 3496
Einzelheiten zur Richtlinie 3496
Version der Richtlinie 3496
JSON-Richtliniendokument 3497
Weitere Informationen 3499

AWSSystemsManagerEnableExplorerExecutionPolicy 3499
Diese Richtlinie wird verwendet 3499
Einzelheiten zur Richtlinie 3499
Version der Richtlinie 3499
JSON-Richtliniendokument 3500
Weitere Informationen 3501
AWSSystemsManagerForSAPFullAccess 3501
Diese Richtlinie wird verwendet 3501
Einzelheiten zur Richtlinie 3501
Version der Richtlinie 3502
JSON-Richtliniendokument 3502
Weitere Informationen 3503
AWSSystemsManagerForSAPReadOnlyAccess 3503
Diese Richtlinie wird verwendet 3503
Einzelheiten zur Richtlinie 3503
Version der Richtlinie 3504
JSON-Richtliniendokument 3504
Weitere Informationen 3504
AWSSystemsManagerJustInTimeAccessServicePolicy 3504
Diese Richtlinie wird verwendet 3505
Einzelheiten der Richtlinie 3505
Version der Richtlinie 3505
JSON-Richtliniendokument 3505
Weitere Informationen 3510
AWSSystemsManagerJustInTimeAccessTokenPolicy 3511
Diese Richtlinie wird verwendet 3511
Einzelheiten zur Richtlinie 3511
Version der Richtlinie 3511
JSON-Richtliniendokument 3511
Weitere Informationen 3514
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy 3514
Diese Richtlinie wird verwendet 3515
Einzelheiten zur Richtlinie 3515
Version der Richtlinie 3515
JSON-Richtliniendokument 3515
Weitere Informationen 3518

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy 3518
Diese Richtlinie wird verwendet 3518
Einzelheiten zur Richtlinie 3518
Version der Richtlinie 3519
JSON-Richtliniendokument 3519
Weitere Informationen 3523
AWSSystemsManagerNotificationsServicePolicy 3523
Diese Richtlinie wird verwendet 3523
Einzelheiten der Richtlinie 3523
Version der Richtlinie 3524
JSON-Richtliniendokument 3524
Weitere Informationen 3525
AWSSystemsManagerOpsDataSyncServiceRolePolicy 3525
Diese Richtlinie wird verwendet 3525
Einzelheiten der Richtlinie 3526
Version der Richtlinie 3526
JSON-Richtliniendokument 3526
Weitere Informationen 3530
AWSThinkboxAssetServerPolicy 3530
Diese Richtlinie wird verwendet 3530
Einzelheiten zur Richtlinie 3530
Version der Richtlinie 3530
JSON-Richtliniendokument 3530
Weitere Informationen 3531
AWSThinkboxAWSPortalAdminPolicy 3531
Diese Richtlinie wird verwendet 3532
Einzelheiten zur Richtlinie 3532
Version der Richtlinie 3532
JSON-Richtliniendokument 3532
Weitere Informationen 3542
AWSThinkboxAWSPortalGatewayPolicy 3542
Diese Richtlinie wird verwendet 3542
Einzelheiten zur Richtlinie 3542
Version der Richtlinie 3543
JSON-Richtliniendokument 3543
Weitere Informationen 3545

AWSThinkboxAWSPortalWorkerPolicy 3545
Diese Richtlinie wird verwendet 3545
Einzelheiten zur Richtlinie 3545
Version der Richtlinie 3545
JSON-Richtliniendokument 3546
Weitere Informationen 3548
AWSThinkboxDeadlineResourceTrackerAccessPolicy 3548
Diese Richtlinie wird verwendet 3548
Einzelheiten zur Richtlinie 3548
Version der Richtlinie 3548
JSON-Richtliniendokument 3549
Weitere Informationen 3551
AWSThinkboxDeadlineResourceTrackerAdminPolicy 3552
Diese Richtlinie wird verwendet 3552
Einzelheiten zur Richtlinie 3552
Version der Richtlinie 3552
JSON-Richtliniendokument 3552
Weitere Informationen 3558
AWSThinkboxDeadlineSpotEventPluginAdminPolicy 3558
Diese Richtlinie wird verwendet 3559
Einzelheiten zur Richtlinie 3559
Version der Richtlinie 3559
JSON-Richtliniendokument 3559
Weitere Informationen 3562
AWSThinkboxDeadlineSpotEventPluginWorkerPolicy 3562
Diese Richtlinie wird verwendet 3562
Einzelheiten zur Richtlinie 3562
Version der Richtlinie 3563
JSON-Richtliniendokument 3563
Weitere Informationen 3564
AWSTransferConsoleFullAccess 3564
Diese Richtlinie wird verwendet 3565
Einzelheiten zur Richtlinie 3565
Version der Richtlinie 3565
JSON-Richtliniendokument 3565
Weitere Informationen 3566

AWSTransferFullAccess 3566
Diese Richtlinie wird verwendet 3566
Einzelheiten zur Richtlinie 3566
Version der Richtlinie 3567
JSON-Richtliniendokument 3567
Weitere Informationen 3568
AWSTransferLoggingAccess 3568
Diese Richtlinie wird verwendet 3568
Einzelheiten zur Richtlinie 3568
Version der Richtlinie 3568
JSON-Richtliniendokument 3569
Weitere Informationen 3569
AWSTransferReadOnlyAccess 3569
Diese Richtlinie wird verwendet 3569
Einzelheiten zur Richtlinie 3570
Version der Richtlinie 3570
JSON-Richtliniendokument 3570
Weitere Informationen 3570
AWSTransformApplicationDeploymentPolicy 3571
Diese Richtlinie wird verwendet 3571
Einzelheiten zur Richtlinie 3571
Version der Richtlinie 3571
JSON-Richtliniendokument 3572
Weitere Informationen 3579
AWSTransformApplicationECSDeploymentPolicy 3580
Diese Richtlinie wird verwendet 3580
Einzelheiten zur Richtlinie 3580
Version der Richtlinie 3580
JSON-Richtliniendokument 3581
Weitere Informationen 3588
AWSTransformCustomExecuteTransformations 3589
Diese Richtlinie wird verwendet 3589
Einzelheiten zur Richtlinie 3589
Version der Richtlinie 3589
JSON-Richtliniendokument 3589
Weitere Informationen 3590

AWSTransformCustomFullAccess 3590
Diese Richtlinie wird verwendet 3590
Einzelheiten zur Richtlinie 3590
Version der Richtlinie 3591
JSON-Richtliniendokument 3591
Weitere Informationen 3591
AWSTransformCustomManageTransformations 3591
Diese Richtlinie wird verwendet 3592
Einzelheiten zur Richtlinie 3592
Version der Richtlinie 3592
JSON-Richtliniendokument 3592
Weitere Informationen 3593
AWSTrustedAdvisorPriorityFullAccess 3593
Diese Richtlinie wird verwendet 3593
Einzelheiten zur Richtlinie 3594
Version der Richtlinie 3594
JSON-Richtliniendokument 3594
Weitere Informationen 3596
AWSTrustedAdvisorPriorityReadOnlyAccess 3596
Diese Richtlinie wird verwendet 3596
Einzelheiten zur Richtlinie 3596
Version der Richtlinie 3596
JSON-Richtliniendokument 3597
Weitere Informationen 3598
AWSTrustedAdvisorReportingServiceRolePolicy 3598
Diese Richtlinie wird verwendet 3598
Einzelheiten der Richtlinie 3598
Version der Richtlinie 3598
JSON-Richtliniendokument 3599
Weitere Informationen 3599
AWSTrustedAdvisorServiceRolePolicy 3599
Diese Richtlinie wird verwendet 3600
Einzelheiten der Richtlinie 3600
Version der Richtlinie 3600
JSON-Richtliniendokument 3600
Weitere Informationen 3603

AWSUserAttributeCostAllocationPolicy 3603
Diese Richtlinie wird verwendet 3603
Einzelheiten der Richtlinie 3604
Version der Richtlinie 3604
JSON-Richtliniendokument 3604
Weitere Informationen 3604
AWSUserNotificationsServiceLinkedRolePolicy 3605
Diese Richtlinie wird verwendet 3605
Einzelheiten der Richtlinie 3605
Version der Richtlinie 3605
JSON-Richtliniendokument 3605
Weitere Informationen 3607
AWSVendorInsightsAssessorFullAccess 3607
Diese Richtlinie wird verwendet 3607
Einzelheiten zur Richtlinie 3607
Version der Richtlinie 3608
JSON-Richtliniendokument 3608
Weitere Informationen 3609
AWSVendorInsightsAssessorReadOnly 3609
Diese Richtlinie wird verwendet 3609
Einzelheiten zur Richtlinie 3609
Version der Richtlinie 3610
JSON-Richtliniendokument 3610
Weitere Informationen 3611
AWSVendorInsightsVendorFullAccess 3611
Diese Richtlinie wird verwendet 3611
Einzelheiten zur Richtlinie 3611
Version der Richtlinie 3611
JSON-Richtliniendokument 3612
Weitere Informationen 3613
AWSVendorInsightsVendorReadOnly 3613
Diese Richtlinie wird verwendet 3614
Einzelheiten zur Richtlinie 3614
Version der Richtlinie 3614
JSON-Richtliniendokument 3614
Weitere Informationen 3615

AWSVpcLatticeServiceRolePolicy 3615
Diese Richtlinie wird verwendet 3616
Einzelheiten der Richtlinie 3616
Version der Richtlinie 3616
JSON-Richtliniendokument 3616
Weitere Informationen 3619
AWSVPCS2SVpnServiceRolePolicy 3619
Diese Richtlinie wird verwendet 3619
Einzelheiten der Richtlinie 3619
Version der Richtlinie 3620
JSON-Richtliniendokument 3620
Weitere Informationen 3621
AWSVPCTransitGatewayServiceRolePolicy 3621
Diese Richtlinie wird verwendet 3621
Einzelheiten der Richtlinie 3621
Version der Richtlinie 3622
JSON-Richtliniendokument 3622
Weitere Informationen 3622
AWSVPCVerifiedAccessServiceRolePolicy 3623
Diese Richtlinie wird verwendet 3623
Einzelheiten der Richtlinie 3623
Version der Richtlinie 3623
JSON-Richtliniendokument 3623
Weitere Informationen 3625
AWSWAFConsoleFullAccess 3625
Diese Richtlinie wird verwendet 3625
Einzelheiten zur Richtlinie 3625
Version der Richtlinie 3626
JSON-Richtliniendokument 3626
Weitere Informationen 3634
AWSWAFConsoleReadOnlyAccess 3635
Diese Richtlinie wird verwendet 3635
Einzelheiten zur Richtlinie 3635
Version der Richtlinie 3635
JSON-Richtliniendokument 3635
Weitere Informationen 3642

AWSWAFFullAccess 3642
Diese Richtlinie wird verwendet 3642
Einzelheiten zur Richtlinie 3643
Version der Richtlinie 3643
JSON-Richtliniendokument 3643
Weitere Informationen 3648
AWSWAFReadOnlyAccess 3648
Diese Richtlinie wird verwendet 3648
Einzelheiten zur Richtlinie 3648
Version der Richtlinie 3649
JSON-Richtliniendokument 3649
Weitere Informationen 3652
AWSWellArchitectedDiscoveryServiceRolePolicy 3652
Diese Richtlinie wird verwendet 3652
Einzelheiten der Richtlinie 3652
Version der Richtlinie 3653
JSON-Richtliniendokument 3653
Weitere Informationen 3654
AWSWellArchitectedOrganizationsServiceRolePolicy 3655
Diese Richtlinie wird verwendet 3655
Einzelheiten der Richtlinie 3655
Version der Richtlinie 3655
JSON-Richtliniendokument 3655
Weitere Informationen 3656
AWSWickrFullAccess 3656
Diese Richtlinie wird verwendet 3656
Einzelheiten zur Richtlinie 3656
Version der Richtlinie 3657
JSON-Richtliniendokument 3657
Weitere Informationen 3657
AWSXrayCrossAccountSharingConfiguration 3657
Diese Richtlinie wird verwendet 3658
Einzelheiten zur Richtlinie 3658
Version der Richtlinie 3658
JSON-Richtliniendokument 3658
Weitere Informationen 3659

AWSXRayDaemonWriteAccess 3659
Diese Richtlinie wird verwendet 3659
Einzelheiten zur Richtlinie 3659
Version der Richtlinie 3660
JSON-Richtliniendokument 3660
Weitere Informationen 3660
AWSXrayFullAccess 3661
Diese Richtlinie wird verwendet 3661
Einzelheiten zur Richtlinie 3661
Version der Richtlinie 3661
JSON-Richtliniendokument 3661
Weitere Informationen 3662
AWSXrayReadOnlyAccess 3662
Diese Richtlinie wird verwendet 3662
Einzelheiten zur Richtlinie 3662
Version der Richtlinie 3662
JSON-Richtliniendokument 3663
Weitere Informationen 3664
AWSXrayWriteOnlyAccess 3664
Diese Richtlinie wird verwendet 3664
Einzelheiten zur Richtlinie 3664
Version der Richtlinie 3664
JSON-Richtliniendokument 3664
Weitere Informationen 3665
AWSZonalAutoshiftPracticeRunSLRPolicy 3665
Diese Richtlinie wird verwendet 3665
Einzelheiten der Richtlinie 3666
Version der Richtlinie 3666
JSON-Richtliniendokument 3666
Weitere Informationen 3667
AWSZoneGroupAccessManagementServiceRolePolicy 3667
Diese Richtlinie wird verwendet 3667
Einzelheiten der Richtlinie 3667
Version der Richtlinie 3668
JSON-Richtliniendokument 3668
Weitere Informationen 3668

BatchServiceRolePolicy 3669
Diese Richtlinie wird verwendet 3669
Einzelheiten der Richtlinie 3669
Version der Richtlinie 3669
JSON-Richtliniendokument 3669
Weitere Informationen 3675
BedrockAgentCoreFullAccess 3676
Diese Richtlinie wird verwendet 3676
Einzelheiten zur Richtlinie 3676
Version der Richtlinie 3676
JSON-Richtliniendokument 3676
Weitere Informationen 3685
BedrockAgentCoreNetworkServiceRolePolicy 3686
Diese Richtlinie wird verwendet 3686
Einzelheiten der Richtlinie 3686
Version der Richtlinie 3686
JSON-Richtliniendokument 3686
Weitere Informationen 3688
BedrockAgentCoreRuntimeIdentityServiceRolePolicy 3688
Diese Richtlinie wird verwendet 3689
Einzelheiten der Richtlinie 3689
Version der Richtlinie 3689
JSON-Richtliniendokument 3689
Weitere Informationen 3690
Billing 3690
Diese Richtlinie wird verwendet 3690
Einzelheiten zur Richtlinie 3690
Version der Richtlinie 3690
JSON-Richtliniendokument 3691
Weitere Informationen 3694
BudgetsServiceRolePolicy 3695
Diese Richtlinie wird verwendet 3695
Einzelheiten der Richtlinie 3695
Version der Richtlinie 3695
JSON-Richtliniendokument 3695
Weitere Informationen 3696

CertificateManagerServiceRolePolicy 3696
Diese Richtlinie wird verwendet 3696
Einzelheiten der Richtlinie 3696
Version der Richtlinie 3696
JSON-Richtliniendokument 3697
Weitere Informationen 3697
ClientVPNServiceConnectionsRolePolicy 3697
Diese Richtlinie wird verwendet 3697
Einzelheiten der Richtlinie 3698
Version der Richtlinie 3698
JSON-Richtliniendokument 3698
Weitere Informationen 3698
ClientVPNServiceRolePolicy 3699
Diese Richtlinie wird verwendet 3699
Einzelheiten der Richtlinie 3699
Version der Richtlinie 3699
JSON-Richtliniendokument 3699
Weitere Informationen 3700
CloudFormationStackSetsOrgAdminServiceRolePolicy 3700
Diese Richtlinie wird verwendet 3701
Einzelheiten der Richtlinie 3701
Version der Richtlinie 3701
JSON-Richtliniendokument 3701
Weitere Informationen 3702
CloudFormationStackSetsOrgMemberServiceRolePolicy 3702
Diese Richtlinie wird verwendet 3702
Einzelheiten der Richtlinie 3702
Version der Richtlinie 3702
JSON-Richtliniendokument 3703
Weitere Informationen 3703
CloudFrontFullAccess 3704
Diese Richtlinie wird verwendet 3704
Einzelheiten zur Richtlinie 3704
Version der Richtlinie 3704
JSON-Richtliniendokument 3704
Weitere Informationen 3706

CloudFrontReadOnlyAccess 3707
Diese Richtlinie wird verwendet 3707
Einzelheiten zur Richtlinie 3707
Version der Richtlinie 3707
JSON-Richtliniendokument 3707
Weitere Informationen 3708
CloudHSMServiceRolePolicy 3708
Diese Richtlinie wird verwendet 3708
Einzelheiten der Richtlinie 3709
Version der Richtlinie 3709
JSON-Richtliniendokument 3709
Weitere Informationen 3709
CloudSearchFullAccess 3710
Diese Richtlinie wird verwendet 3710
Einzelheiten zur Richtlinie 3710
Version der Richtlinie 3710
JSON-Richtliniendokument 3710
Weitere Informationen 3711
CloudSearchReadOnlyAccess 3711
Diese Richtlinie wird verwendet 3711
Einzelheiten zur Richtlinie 3711
Version der Richtlinie 3711
JSON-Richtliniendokument 3712
Weitere Informationen 3712
CloudTrailEventContext 3712
Diese Richtlinie wird verwendet 3712
Einzelheiten der Richtlinie 3713
Version der Richtlinie 3713
JSON-Richtliniendokument 3713
Weitere Informationen 3715
CloudTrailServiceRolePolicy 3715
Diese Richtlinie wird verwendet 3715
Einzelheiten der Richtlinie 3715
Version der Richtlinie 3715
JSON-Richtliniendokument 3716
Weitere Informationen 3717

CloudWatch-CrossAccountAccess 3717
Diese Richtlinie wird verwendet 3718
Einzelheiten der Richtlinie 3718
Version der Richtlinie 3718
JSON-Richtliniendokument 3718
Weitere Informationen 3719
CloudWatchActionsEC2Access 3719
Diese Richtlinie wird verwendet 3719
Einzelheiten zur Richtlinie 3719
Version der Richtlinie 3719
JSON-Richtliniendokument 3719
Weitere Informationen 3720
CloudWatchAgentAdminPolicy 3720
Diese Richtlinie wird verwendet 3720
Einzelheiten zur Richtlinie 3720
Version der Richtlinie 3721
JSON-Richtliniendokument 3721
Weitere Informationen 3722
CloudWatchAgentServerPolicy 3722
Diese Richtlinie wird verwendet 3722
Einzelheiten zur Richtlinie 3722
Version der Richtlinie 3722
JSON-Richtliniendokument 3723
Weitere Informationen 3723
CloudWatchApplicationInsightsFullAccess 3724
Diese Richtlinie wird verwendet 3724
Einzelheiten zur Richtlinie 3724
Version der Richtlinie 3724
JSON-Richtliniendokument 3724
Weitere Informationen 3726
CloudWatchApplicationInsightsReadOnlyAccess 3726
Diese Richtlinie wird verwendet 3726
Einzelheiten zur Richtlinie 3726
Version der Richtlinie 3726
JSON-Richtliniendokument 3727
Weitere Informationen 3727

CloudwatchApplicationInsightsServiceLinkedRolePolicy 3727
Diese Richtlinie wird verwendet 3727
Einzelheiten der Richtlinie 3728
Version der Richtlinie 3728
JSON-Richtliniendokument 3728
Weitere Informationen 3739
CloudWatchApplicationSignalsFullAccess 3739
Diese Richtlinie wird verwendet 3739
Einzelheiten zur Richtlinie 3739
Version der Richtlinie 3739
JSON-Richtliniendokument 3740
Weitere Informationen 3745
CloudWatchApplicationSignalsReadOnlyAccess 3745
Diese Richtlinie wird verwendet 3745
Einzelheiten zur Richtlinie 3745
Version der Richtlinie 3745
JSON-Richtliniendokument 3746
Weitere Informationen 3750
CloudWatchApplicationSignalsServiceRolePolicy 3750
Diese Richtlinie wird verwendet 3750
Einzelheiten der Richtlinie 3750
Version der Richtlinie 3751
JSON-Richtliniendokument 3751
Weitere Informationen 3754
CloudWatchAutomaticDashboardsAccess 3754
Diese Richtlinie wird verwendet 3754
Einzelheiten zur Richtlinie 3754
Version der Richtlinie 3754
JSON-Richtliniendokument 3755
Weitere Informationen 3756
CloudWatchCrossAccountSharingConfiguration 3756
Diese Richtlinie wird verwendet 3756
Einzelheiten zur Richtlinie 3757
Version der Richtlinie 3757
JSON-Richtliniendokument 3757
Weitere Informationen 3758

CloudWatchEventsBuiltInTargetExecutionAccess 3758
Diese Richtlinie wird verwendet 3758
Einzelheiten zur Richtlinie 3758
Version der Richtlinie 3759
JSON-Richtliniendokument 3759
Weitere Informationen 3759
CloudWatchEventsFullAccess 3760
Diese Richtlinie wird verwendet 3760
Einzelheiten zur Richtlinie 3760
Version der Richtlinie 3760
JSON-Richtliniendokument 3760
Weitere Informationen 3762
CloudWatchEventsInvocationAccess 3762
Diese Richtlinie wird verwendet 3763
Einzelheiten zur Richtlinie 3763
Version der Richtlinie 3763
JSON-Richtliniendokument 3763
Weitere Informationen 3764
CloudWatchEventsReadOnlyAccess 3764
Diese Richtlinie wird verwendet 3764
Einzelheiten zur Richtlinie 3764
Version der Richtlinie 3764
JSON-Richtliniendokument 3764
Weitere Informationen 3766
CloudWatchEventsServiceRolePolicy 3766
Diese Richtlinie wird verwendet 3766
Einzelheiten der Richtlinie 3766
Version der Richtlinie 3767
JSON-Richtliniendokument 3767
Weitere Informationen 3767
CloudWatchFullAccess 3768
Diese Richtlinie wird verwendet 3768
Einzelheiten zur Richtlinie 3768
Version der Richtlinie 3768
JSON-Richtliniendokument 3768
Weitere Informationen 3769

CloudWatchFullAccessV2 3769
Diese Richtlinie wird verwendet 3770
Einzelheiten zur Richtlinie 3770
Version der Richtlinie 3770
JSON-Richtliniendokument 3770
Weitere Informationen 3775
CloudWatchInternetMonitorFullAccess 3776
Diese Richtlinie wird verwendet 3776
Einzelheiten zur Richtlinie 3776
Version der Richtlinie 3776
JSON-Richtliniendokument 3776
Weitere Informationen 3778
CloudWatchInternetMonitorReadOnlyAccess 3778
Diese Richtlinie wird verwendet 3779
Einzelheiten zur Richtlinie 3779
Version der Richtlinie 3779
JSON-Richtliniendokument 3779
Weitere Informationen 3780
CloudWatchInternetMonitorServiceRolePolicy 3780
Diese Richtlinie wird verwendet 3780
Einzelheiten der Richtlinie 3780
Version der Richtlinie 3781
JSON-Richtliniendokument 3781
Weitere Informationen 3782
CloudWatchLambdaApplicationSignalsExecutionRolePolicy 3782
Diese Richtlinie wird verwendet 3782
Einzelheiten zur Richtlinie 3782
Version der Richtlinie 3783
JSON-Richtliniendokument 3783
Weitere Informationen 3784
CloudWatchLambdaInsightsExecutionRolePolicy 3784
Diese Richtlinie wird verwendet 3784
Einzelheiten zur Richtlinie 3784
Version der Richtlinie 3784
JSON-Richtliniendokument 3785
Weitere Informationen 3785

CloudWatchLogsCrossAccountSharingConfiguration 3785
Diese Richtlinie wird verwendet 3786
Einzelheiten zur Richtlinie 3786
Version der Richtlinie 3786
JSON-Richtliniendokument 3786
Weitere Informationen 3787
CloudWatchLogsFullAccess 3787
Diese Richtlinie wird verwendet 3787
Einzelheiten zur Richtlinie 3788
Version der Richtlinie 3788
JSON-Richtliniendokument 3788
Weitere Informationen 3789
CloudWatchLogsReadOnlyAccess 3789
Diese Richtlinie wird verwendet 3789
Einzelheiten zur Richtlinie 3789
Version der Richtlinie 3789
JSON-Richtliniendokument 3789
Weitere Informationen 3790
CloudWatchNetworkFlowMonitorAgentPublishPolicy 3790
Diese Richtlinie wird verwendet 3791
Einzelheiten zur Richtlinie 3791
Version der Richtlinie 3791
JSON-Richtliniendokument 3791
Weitere Informationen 3792
CloudWatchNetworkFlowMonitorServiceRolePolicy 3792
Diese Richtlinie wird verwendet 3792
Einzelheiten der Richtlinie 3792
Version der Richtlinie 3792
JSON-Richtliniendokument 3793
Weitere Informationen 3794
CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy 3794
Diese Richtlinie wird verwendet 3794
Einzelheiten der Richtlinie 3794
Version der Richtlinie 3794
JSON-Richtliniendokument 3795
Weitere Informationen 3796

CloudWatchNetworkMonitorServiceRolePolicy 3796
Diese Richtlinie wird verwendet 3796
Einzelheiten der Richtlinie 3796
Version der Richtlinie 3796
JSON-Richtliniendokument 3797
Weitere Informationen 3798
CloudWatchOpenSearchDashboardAccess 3798
Diese Richtlinie wird verwendet 3798
Einzelheiten zur Richtlinie 3798
Version der Richtlinie 3799
JSON-Richtliniendokument 3799
Weitere Informationen 3801
CloudWatchOpenSearchDashboardsFullAccess 3802
Diese Richtlinie wird verwendet 3802
Einzelheiten zur Richtlinie 3802
Version der Richtlinie 3802
JSON-Richtliniendokument 3802
Weitere Informationen 3809
CloudWatchReadOnlyAccess 3809
Diese Richtlinie wird verwendet 3810
Einzelheiten zur Richtlinie 3810
Version der Richtlinie 3810
JSON-Richtliniendokument 3810
Weitere Informationen 3813
CloudWatchSyntheticsFullAccess 3813
Diese Richtlinie wird verwendet 3813
Einzelheiten zur Richtlinie 3813
Version der Richtlinie 3814
JSON-Richtliniendokument 3814
Weitere Informationen 3819
CloudWatchSyntheticsReadOnlyAccess 3819
Diese Richtlinie wird verwendet 3819
Einzelheiten zur Richtlinie 3819
Version der Richtlinie 3820
JSON-Richtliniendokument 3820
Weitere Informationen 3820

ComprehendDataAccessRolePolicy 3821
Diese Richtlinie wird verwendet 3821
Einzelheiten zur Richtlinie 3821
Version der Richtlinie 3821
JSON-Richtliniendokument 3821
Weitere Informationen 3822
ComprehendFullAccess 3822
Diese Richtlinie wird verwendet 3822
Einzelheiten zur Richtlinie 3822
Version der Richtlinie 3822
JSON-Richtliniendokument 3823
Weitere Informationen 3823
ComprehendMedicalFullAccess 3823
Diese Richtlinie wird verwendet 3823
Einzelheiten zur Richtlinie 3824
Version der Richtlinie 3824
JSON-Richtliniendokument 3824
Weitere Informationen 3824
ComprehendReadOnly 3825
Diese Richtlinie wird verwendet 3825
Einzelheiten zur Richtlinie 3825
Version der Richtlinie 3825
JSON-Richtliniendokument 3825
Weitere Informationen 3826
ComputeOptimizerAutomationServiceRolePolicy 3827
Diese Richtlinie wird verwendet 3827
Einzelheiten der Richtlinie 3827
Version der Richtlinie 3827
JSON-Richtliniendokument 3828
Weitere Informationen 3829
ComputeOptimizerReadOnlyAccess 3829
Diese Richtlinie wird verwendet 3830
Einzelheiten zur Richtlinie 3830
Version der Richtlinie 3830
JSON-Richtliniendokument 3830
Weitere Informationen 3831

ComputeOptimizerServiceRolePolicy 3831
Diese Richtlinie wird verwendet 3832
Einzelheiten der Richtlinie 3832
Version der Richtlinie 3832
JSON-Richtliniendokument 3832
Weitere Informationen 3834
ConfigConformsServiceRolePolicy 3834
Diese Richtlinie wird verwendet 3834
Einzelheiten der Richtlinie 3834
Version der Richtlinie 3834
JSON-Richtliniendokument 3835
Weitere Informationen 3837
ConsoleFullAccessFromVercel 3838
Diese Richtlinie wird verwendet 3838
Einzelheiten zur Richtlinie 3838
Version der Richtlinie 3838
JSON-Richtliniendokument 3838
Weitere Informationen 3842
ConsoleViewOnlyAccessFromVercel 3842
Diese Richtlinie wird verwendet 3842
Einzelheiten zur Richtlinie 3843
Version der Richtlinie 3843
JSON-Richtliniendokument 3843
Weitere Informationen 3845
CostOptimizationHubAdminAccess 3845
Diese Richtlinie wird verwendet 3845
Einzelheiten zur Richtlinie 3845
Version der Richtlinie 3845
JSON-Richtliniendokument 3846
Weitere Informationen 3847
CostOptimizationHubReadOnlyAccess 3847
Diese Richtlinie wird verwendet 3847
Einzelheiten zur Richtlinie 3847
Version der Richtlinie 3848
JSON-Richtliniendokument 3848
Weitere Informationen 3848

CostOptimizationHubServiceRolePolicy 3849
Diese Richtlinie wird verwendet 3849
Einzelheiten der Richtlinie 3849
Version der Richtlinie 3849
JSON-Richtliniendokument 3849
Weitere Informationen 3850
CustomerProfilesServiceLinkedRolePolicy 3851
Diese Richtlinie wird verwendet 3851
Einzelheiten der Richtlinie 3851
Version der Richtlinie 3851
JSON-Richtliniendokument 3851
Weitere Informationen 3852
DatabaseAdministrator 3853
Diese Richtlinie wird verwendet 3853
Einzelheiten zur Richtlinie 3853
Version der Richtlinie 3853
JSON-Richtliniendokument 3853
Weitere Informationen 3856
DataScientist 3856
Diese Richtlinie wird verwendet 3856
Einzelheiten zur Richtlinie 3856
Version der Richtlinie 3857
JSON-Richtliniendokument 3857
Weitere Informationen 3861
DAXServiceRolePolicy 3861
Diese Richtlinie wird verwendet 3861
Einzelheiten der Richtlinie 3861
Version der Richtlinie 3861
JSON-Richtliniendokument 3862
Weitere Informationen 3862
DeclarativePoliciesEC2Report 3862
Diese Richtlinie wird verwendet 3863
Einzelheiten der Richtlinie 3863
Version der Richtlinie 3863
JSON-Richtliniendokument 3863
Weitere Informationen 3864

DynamoDBCloudWatchContributorInsightsServiceRolePolicy 3864
Diese Richtlinie wird verwendet 3864
Einzelheiten der Richtlinie 3864
Version der Richtlinie 3865
JSON-Richtliniendokument 3865
Weitere Informationen 3865
DynamoDBGlobalTableSettingsManagementServiceRolePolicy 3866
Diese Richtlinie wird verwendet 3866
Einzelheiten der Richtlinie 3866
Version der Richtlinie 3866
JSON-Richtliniendokument 3866
Weitere Informationen 3867
DynamoDBKinesisReplicationServiceRolePolicy 3868
Diese Richtlinie wird verwendet 3868
Einzelheiten der Richtlinie 3868
Version der Richtlinie 3868
JSON-Richtliniendokument 3868
Weitere Informationen 3869
DynamoDBReplicationServiceRolePolicy 3869
Diese Richtlinie wird verwendet 3869
Einzelheiten der Richtlinie 3870
Version der Richtlinie 3870
JSON-Richtliniendokument 3870
Weitere Informationen 3871
EC2FastLaunchFullAccess 3871
Diese Richtlinie wird verwendet 3871
Einzelheiten zur Richtlinie 3872
Version der Richtlinie 3872
JSON-Richtliniendokument 3872
Weitere Informationen 3879
EC2FastLaunchServiceRolePolicy 3879
Diese Richtlinie wird verwendet 3879
Einzelheiten der Richtlinie 3879
Version der Richtlinie 3880
JSON-Richtliniendokument 3880
Weitere Informationen 3886

EC2FleetTimeShiftableServiceRolePolicy 3886
Diese Richtlinie wird verwendet 3886
Einzelheiten der Richtlinie 3886
Version der Richtlinie 3887
JSON-Richtliniendokument 3887
Weitere Informationen 3888
Ec2ImageBuilderCrossAccountDistributionAccess 3888
Diese Richtlinie wird verwendet 3889
Einzelheiten zur Richtlinie 3889
Version der Richtlinie 3889
JSON-Richtliniendokument 3889
Weitere Informationen 3890
EC2ImageBuilderLifecycleExecutionPolicy 3890
Diese Richtlinie wird verwendet 3890
Einzelheiten zur Richtlinie 3890
Version der Richtlinie 3890
JSON-Richtliniendokument 3891
Weitere Informationen 3893
EC2InstanceConnect 3893
Diese Richtlinie wird verwendet 3893
Einzelheiten zur Richtlinie 3893
Version der Richtlinie 3893
JSON-Richtliniendokument 3894
Weitere Informationen 3894
Ec2InstanceConnectEndpoint 3894
Diese Richtlinie wird verwendet 3894
Einzelheiten der Richtlinie 3895
Version der Richtlinie 3895
JSON-Richtliniendokument 3895
Weitere Informationen 3898
EC2InstanceProfileForImageBuilder 3898
Diese Richtlinie wird verwendet 3898
Einzelheiten zur Richtlinie 3898
Version der Richtlinie 3898
JSON-Richtliniendokument 3898
Weitere Informationen 3901

EC2InstanceProfileForImageBuilderECRContainerBuilds 3901
Diese Richtlinie wird verwendet 3902
Einzelheiten zur Richtlinie 3902
Version der Richtlinie 3902
JSON-Richtliniendokument 3902
Weitere Informationen 3903
ECRReplicationServiceRolePolicy 3904
Diese Richtlinie wird verwendet 3904
Einzelheiten der Richtlinie 3904
Version der Richtlinie 3904
JSON-Richtliniendokument 3904
Weitere Informationen 3905
ECRTemplateServiceRolePolicy 3905
Diese Richtlinie wird verwendet 3905
Einzelheiten der Richtlinie 3905
Version der Richtlinie 3906
JSON-Richtliniendokument 3906
Weitere Informationen 3906
ElastiCacheServiceRolePolicy 3906
Diese Richtlinie wird verwendet 3907
Einzelheiten der Richtlinie 3907
Version der Richtlinie 3907
JSON-Richtliniendokument 3907
Weitere Informationen 3909
ElasticLoadBalancingFullAccess 3909
Diese Richtlinie wird verwendet 3909
Einzelheiten zur Richtlinie 3910
Version der Richtlinie 3910
JSON-Richtliniendokument 3910
Weitere Informationen 3911
ElasticLoadBalancingReadOnly 3912
Diese Richtlinie wird verwendet 3912
Einzelheiten zur Richtlinie 3912
Version der Richtlinie 3912
JSON-Richtliniendokument 3912
Weitere Informationen 3913

ElementalActivationsDownloadSoftwareAccess 3914
Diese Richtlinie wird verwendet 3914
Einzelheiten zur Richtlinie 3914
Version der Richtlinie 3914
JSON-Richtliniendokument 3914
Weitere Informationen 3915
ElementalActivationsFullAccess 3915
Diese Richtlinie wird verwendet 3915
Einzelheiten zur Richtlinie 3915
Version der Richtlinie 3915
JSON-Richtliniendokument 3916
Weitere Informationen 3916
ElementalActivationsGenerateLicenses 3916
Diese Richtlinie wird verwendet 3916
Einzelheiten zur Richtlinie 3917
Version der Richtlinie 3917
JSON-Richtliniendokument 3917
Weitere Informationen 3917
ElementalActivationsReadOnlyAccess 3918
Diese Richtlinie wird verwendet 3918
Einzelheiten zur Richtlinie 3918
Version der Richtlinie 3918
JSON-Richtliniendokument 3918
Weitere Informationen 3919
ElementalAppliancesSoftwareFullAccess 3919
Diese Richtlinie wird verwendet 3919
Einzelheiten zur Richtlinie 3919
Version der Richtlinie 3920
JSON-Richtliniendokument 3920
Weitere Informationen 3920
ElementalAppliancesSoftwareReadOnlyAccess 3920
Diese Richtlinie wird verwendet 3921
Einzelheiten zur Richtlinie 3921
Version der Richtlinie 3921
JSON-Richtliniendokument 3921
Weitere Informationen 3922

ElementalSupportCenterFullAccess 3922
Diese Richtlinie wird verwendet 3922
Einzelheiten zur Richtlinie 3922
Version der Richtlinie 3922
JSON-Richtliniendokument 3923
Weitere Informationen 3923
EMRDescribeClusterPolicyForEMRWAL 3923
Diese Richtlinie wird verwendet 3923
Einzelheiten der Richtlinie 3924
Version der Richtlinie 3924
JSON-Richtliniendokument 3924
Weitere Informationen 3924
FMSServiceRolePolicy 3925
Diese Richtlinie wird verwendet 3925
Einzelheiten der Richtlinie 3925
Version der Richtlinie 3925
JSON-Richtliniendokument 3925
Weitere Informationen 3942
FSxDeleteServiceLinkedRoleAccess 3942
Diese Richtlinie wird verwendet 3942
Einzelheiten der Richtlinie 3942
Version der Richtlinie 3942
JSON-Richtliniendokument 3943
Weitere Informationen 3943
GameLiftContainerFleetPolicy 3943
Diese Richtlinie wird verwendet 3943
Einzelheiten zur Richtlinie 3944
Version der Richtlinie 3944
JSON-Richtliniendokument 3944
Weitere Informationen 3945
GameLiftGameServerGroupPolicy 3945
Diese Richtlinie wird verwendet 3946
Einzelheiten zur Richtlinie 3946
Version der Richtlinie 3946
JSON-Richtliniendokument 3946
Weitere Informationen 3948

GitLabDuoWithAmazonQPermissionsPolicy 3948
Diese Richtlinie wird verwendet 3948
Einzelheiten zur Richtlinie 3948
Version der Richtlinie 3948
JSON-Richtliniendokument 3949
Weitere Informationen 3950
GlobalAcceleratorFullAccess 3950
Diese Richtlinie wird verwendet 3950
Einzelheiten zur Richtlinie 3950
Version der Richtlinie 3950
JSON-Richtliniendokument 3950
Weitere Informationen 3951
GlobalAcceleratorReadOnlyAccess 3952
Diese Richtlinie wird verwendet 3952
Einzelheiten zur Richtlinie 3952
Version der Richtlinie 3952
JSON-Richtliniendokument 3952
Weitere Informationen 3953
GreengrassOTAUpdateArtifactAccess 3953
Diese Richtlinie wird verwendet 3953
Einzelheiten zur Richtlinie 3953
Version der Richtlinie 3954
JSON-Richtliniendokument 3954
Weitere Informationen 3954
GroundTruthSyntheticConsoleFullAccess 3954
Diese Richtlinie wird verwendet 3955
Einzelheiten zur Richtlinie 3955
Version der Richtlinie 3955
JSON-Richtliniendokument 3955
Weitere Informationen 3956
GroundTruthSyntheticConsoleReadOnlyAccess 3956
Diese Richtlinie wird verwendet 3956
Einzelheiten zur Richtlinie 3956
Version der Richtlinie 3956
JSON-Richtliniendokument 3957
Weitere Informationen 3957

Health_OrganizationsServiceRolePolicy 3957
Diese Richtlinie wird verwendet 3957
Einzelheiten der Richtlinie 3958
Version der Richtlinie 3958
JSON-Richtliniendokument 3958
Weitere Informationen 3959
IAMAccessAdvisorReadOnly 3959
Diese Richtlinie wird verwendet 3959
Einzelheiten zur Richtlinie 3959
Version der Richtlinie 3959
JSON-Richtliniendokument 3959
Weitere Informationen 3960
IAMAccessAnalyzerFullAccess 3961
Diese Richtlinie wird verwendet 3961
Einzelheiten zur Richtlinie 3961
Version der Richtlinie 3961
JSON-Richtliniendokument 3961
Weitere Informationen 3962
IAMAccessAnalyzerReadOnlyAccess 3962
Diese Richtlinie wird verwendet 3963
Einzelheiten zur Richtlinie 3963
Version der Richtlinie 3963
JSON-Richtliniendokument 3963
Weitere Informationen 3964
IAMFullAccess 3964
Diese Richtlinie wird verwendet 3964
Einzelheiten zur Richtlinie 3964
Version der Richtlinie 3964
JSON-Richtliniendokument 3965
Weitere Informationen 3965
IAMReadOnlyAccess 3965
Diese Richtlinie wird verwendet 3966
Einzelheiten zur Richtlinie 3966
Version der Richtlinie 3966
JSON-Richtliniendokument 3966
Weitere Informationen 3967

IAMSelfManageServiceSpecificCredentials 3967
Diese Richtlinie wird verwendet 3967
Einzelheiten zur Richtlinie 3967
Version der Richtlinie 3967
JSON-Richtliniendokument 3968
Weitere Informationen 3968
IAMUserChangePassword 3968
Diese Richtlinie wird verwendet 3968
Einzelheiten zur Richtlinie 3969
Version der Richtlinie 3969
JSON-Richtliniendokument 3969
Weitere Informationen 3970
IAMUserSSHKeys 3970
Diese Richtlinie wird verwendet 3970
Einzelheiten zur Richtlinie 3970
Version der Richtlinie 3970
JSON-Richtliniendokument 3970
Weitere Informationen 3971
IVSFullAccess 3971
Diese Richtlinie wird verwendet 3971
Einzelheiten zur Richtlinie 3971
Version der Richtlinie 3972
JSON-Richtliniendokument 3972
Weitere Informationen 3972
IVSReadOnlyAccess 3973
Diese Richtlinie wird verwendet 3973
Einzelheiten zur Richtlinie 3973
Version der Richtlinie 3973
JSON-Richtliniendokument 3973
Weitere Informationen 3974
IVSRecordToS3 3975
Diese Richtlinie wird verwendet 3975
Einzelheiten der Richtlinie 3975
Version der Richtlinie 3975
JSON-Richtliniendokument 3975
Weitere Informationen 3976

KafkaConnectServiceRolePolicy 3976
Diese Richtlinie wird verwendet 3976
Einzelheiten der Richtlinie 3976
Version der Richtlinie 3976
JSON-Richtliniendokument 3977
Weitere Informationen 3978
KafkaServiceRolePolicy 3978
Diese Richtlinie wird verwendet 3978
Einzelheiten der Richtlinie 3979
Version der Richtlinie 3979
JSON-Richtliniendokument 3979
Weitere Informationen 3981
KeyspacesCDCServiceRolePolicy 3981
Diese Richtlinie wird verwendet 3981
Einzelheiten der Richtlinie 3981
Version der Richtlinie 3982
JSON-Richtliniendokument 3982
Weitere Informationen 3982
KeyspacesReplicationServiceRolePolicy 3982
Diese Richtlinie wird verwendet 3983
Einzelheiten der Richtlinie 3983
Version der Richtlinie 3983
JSON-Richtliniendokument 3983
Weitere Informationen 3985
LakeFormationDataAccessServiceRolePolicy 3985
Diese Richtlinie wird verwendet 3985
Einzelheiten der Richtlinie 3985
Version der Richtlinie 3985
JSON-Richtliniendokument 3986
Weitere Informationen 3986
LexBotPolicy 3986
Diese Richtlinie wird verwendet 3986
Einzelheiten der Richtlinie 3986
Version der Richtlinie 3987
JSON-Richtliniendokument 3987
Weitere Informationen 3988

LexChannelPolicy 3988
Diese Richtlinie wird verwendet 3988
Einzelheiten der Richtlinie 3988
Version der Richtlinie 3988
JSON-Richtliniendokument 3988
Weitere Informationen 3989
LightsailExportAccess 3989
Diese Richtlinie wird verwendet 3989
Einzelheiten der Richtlinie 3989
Version der Richtlinie 3990
JSON-Richtliniendokument 3990
Weitere Informationen 3991
MediaConnectGatewayInstanceRolePolicy 3991
Diese Richtlinie wird verwendet 3991
Einzelheiten zur Richtlinie 3991
Version der Richtlinie 3991
JSON-Richtliniendokument 3991
Weitere Informationen 3992
MediaPackageServiceRolePolicy 3992
Diese Richtlinie wird verwendet 3992
Einzelheiten der Richtlinie 3992
Version der Richtlinie 3993
JSON-Richtliniendokument 3993
Weitere Informationen 3993
MemoryDBServiceRolePolicy 3994
Diese Richtlinie wird verwendet 3994
Einzelheiten der Richtlinie 3994
Version der Richtlinie 3994
JSON-Richtliniendokument 3994
Weitere Informationen 3996
MigrationHubDMSAccessServiceRolePolicy 3997
Diese Richtlinie wird verwendet 3997
Einzelheiten der Richtlinie 3997
Version der Richtlinie 3997
JSON-Richtliniendokument 3997
Weitere Informationen 3998

MigrationHubServiceRolePolicy 3999
Diese Richtlinie wird verwendet 3999
Einzelheiten der Richtlinie 3999
Version der Richtlinie 3999
JSON-Richtliniendokument 3999
Weitere Informationen 4001
MigrationHubSMSAccessServiceRolePolicy 4001
Diese Richtlinie wird verwendet 4001
Einzelheiten der Richtlinie 4001
Version der Richtlinie 4001
JSON-Richtliniendokument 4002
Weitere Informationen 4002
MonitronServiceRolePolicy 4003
Diese Richtlinie wird verwendet 4003
Einzelheiten der Richtlinie 4003
Version der Richtlinie 4003
JSON-Richtliniendokument 4003
Weitere Informationen 4004
MultiPartyApprovalFullAccess 4004
Diese Richtlinie wird verwendet 4004
Einzelheiten zur Richtlinie 4004
Version der Richtlinie 4005
JSON-Richtliniendokument 4005
Weitere Informationen 4007
MultiPartyApprovalReadOnlyAccess 4007
Diese Richtlinie wird verwendet 4008
Einzelheiten zur Richtlinie 4008
Version der Richtlinie 4008
JSON-Richtliniendokument 4008
Weitere Informationen 4010
NeptuneConsoleFullAccess 4010
Diese Richtlinie wird verwendet 4010
Einzelheiten zur Richtlinie 4010
Version der Richtlinie 4011
JSON-Richtliniendokument 4011
Weitere Informationen 4016

NeptuneFullAccess 4017
Diese Richtlinie wird verwendet 4017
Einzelheiten zur Richtlinie 4017
Version der Richtlinie 4017
JSON-Richtliniendokument 4017
Weitere Informationen 4021
NeptuneGraphReadOnlyAccess 4021
Diese Richtlinie wird verwendet 4022
Einzelheiten zur Richtlinie 4022
Version der Richtlinie 4022
JSON-Richtliniendokument 4022
Weitere Informationen 4024
NeptuneReadOnlyAccess 4024
Diese Richtlinie wird verwendet 4024
Einzelheiten zur Richtlinie 4024
Version der Richtlinie 4024
JSON-Richtliniendokument 4025
Weitere Informationen 4027
NetworkAdministrator 4027
Diese Richtlinie wird verwendet 4027
Einzelheiten zur Richtlinie 4027
Version der Richtlinie 4027
JSON-Richtliniendokument 4028
Weitere Informationen 4035
NetworkSecurityDirectorServiceLinkedRolePolicy 4035
Diese Richtlinie wird verwendet 4035
Einzelheiten der Richtlinie 4035
Version der Richtlinie 4035
JSON-Richtliniendokument 4036
Weitere Informationen 4041
NovaActServiceRolePolicy 4041
Diese Richtlinie wird verwendet 4041
Einzelheiten der Richtlinie 4041
Version der Richtlinie 4041
JSON-Richtliniendokument 4042
Weitere Informationen 4042

OAMFullAccess 4042
Diese Richtlinie wird verwendet 4043
Einzelheiten zur Richtlinie 4043
Version der Richtlinie 4043
JSON-Richtliniendokument 4043
Weitere Informationen 4043
OAMReadOnlyAccess 4044
Diese Richtlinie wird verwendet 4044
Einzelheiten zur Richtlinie 4044
Version der Richtlinie 4044
JSON-Richtliniendokument 4044
Weitere Informationen 4045
OpensearchIngestionSelfManagedVpcePolicy 4045
Diese Richtlinie wird verwendet 4045
Einzelheiten der Richtlinie 4045
Version der Richtlinie 4046
JSON-Richtliniendokument 4046
Weitere Informationen 4046
PartnerCentralAccountManagementUserRoleAssociation 4047
Diese Richtlinie wird verwendet 4047
Einzelheiten zur Richtlinie 4047
Version der Richtlinie 4047
JSON-Richtliniendokument 4047
Weitere Informationen 4048
PowerUserAccess 4048
Diese Richtlinie wird verwendet 4049
Einzelheiten zur Richtlinie 4049
Version der Richtlinie 4049
JSON-Richtliniendokument 4049
Weitere Informationen 4050
QAppsServiceRolePolicy 4050
Diese Richtlinie wird verwendet 4050
Einzelheiten der Richtlinie 4050
Version der Richtlinie 4051
JSON-Richtliniendokument 4051
Weitere Informationen 4051

QBusinessQuicksightPluginPolicy 4051
Diese Richtlinie wird verwendet 4052
Einzelheiten zur Richtlinie 4052
Version der Richtlinie 4052
JSON-Richtliniendokument 4052
Weitere Informationen 4053
QBusinessServiceRolePolicy 4053
Diese Richtlinie wird verwendet 4053
Einzelheiten der Richtlinie 4053
Version der Richtlinie 4053
JSON-Richtliniendokument 4054
Weitere Informationen 4055
QuickSightAccessForS3StorageManagementAnalyticsReadOnly 4055
Diese Richtlinie wird verwendet 4056
Einzelheiten zur Richtlinie 4056
Version der Richtlinie 4056
JSON-Richtliniendokument 4056
Weitere Informationen 4057
RDSCloudHsmAuthorizationRole 4057
Diese Richtlinie wird verwendet 4057
Einzelheiten zur Richtlinie 4057
Version der Richtlinie 4057
JSON-Richtliniendokument 4058
Weitere Informationen 4058
ReadOnlyAccess 4058
Diese Richtlinie wird verwendet 4059
Einzelheiten zur Richtlinie 4059
Version der Richtlinie 4059
JSON-Richtliniendokument 4059
Weitere Informationen 4119
ResourceGroupsandTagEditorFullAccess 4119
Diese Richtlinie wird verwendet 4120
Einzelheiten zur Richtlinie 4120
Version der Richtlinie 4120
JSON-Richtliniendokument 4120
Weitere Informationen 4121

ResourceGroupsandTagEditorReadOnlyAccess 4121
Diese Richtlinie wird verwendet 4121
Einzelheiten zur Richtlinie 4121
Version der Richtlinie 4121
JSON-Richtliniendokument 4122
Weitere Informationen 4122
ResourceGroupsServiceRolePolicy 4122
Diese Richtlinie wird verwendet 4123
Einzelheiten der Richtlinie 4123
Version der Richtlinie 4123
JSON-Richtliniendokument 4123
Weitere Informationen 4124
ResourceGroupsTaggingAPITagUntagSupportedResources 4124
Diese Richtlinie wird verwendet 4124
Einzelheiten zur Richtlinie 4124
Version der Richtlinie 4124
JSON-Richtliniendokument 4125
Weitere Informationen 4133
ROSAAmazonEBSCSIDriverOperatorPolicy 4133
Diese Richtlinie wird verwendet 4133
Einzelheiten zur Richtlinie 4133
Version der Richtlinie 4134
JSON-Richtliniendokument 4134
Weitere Informationen 4137
ROSACloudNetworkConfigOperatorPolicy 4137
Diese Richtlinie wird verwendet 4138
Einzelheiten zur Richtlinie 4138
Version der Richtlinie 4138
JSON-Richtliniendokument 4138
Weitere Informationen 4139
ROSAControlPlaneOperatorPolicy 4139
Diese Richtlinie wird verwendet 4139
Einzelheiten zur Richtlinie 4139
Version der Richtlinie 4140
JSON-Richtliniendokument 4140
Weitere Informationen 4144

ROSAImageRegistryOperatorPolicy 4145
Diese Richtlinie wird verwendet 4145
Einzelheiten zur Richtlinie 4145
Version der Richtlinie 4145
JSON-Richtliniendokument 4145
Weitere Informationen 4147
ROSAIngressOperatorPolicy 4147
Diese Richtlinie wird verwendet 4147
Einzelheiten zur Richtlinie 4147
Version der Richtlinie 4147
JSON-Richtliniendokument 4148
Weitere Informationen 4148
ROSAInstallerPolicy 4149
Diese Richtlinie wird verwendet 4149
Einzelheiten zur Richtlinie 4149
Version der Richtlinie 4149
JSON-Richtliniendokument 4149
Weitere Informationen 4158
ROSAKMSProviderPolicy 4158
Diese Richtlinie wird verwendet 4158
Einzelheiten zur Richtlinie 4158
Version der Richtlinie 4158
JSON-Richtliniendokument 4159
Weitere Informationen 4159
ROSAKubeControllerPolicy 4160
Diese Richtlinie wird verwendet 4160
Einzelheiten zur Richtlinie 4160
Version der Richtlinie 4160
JSON-Richtliniendokument 4160
Weitere Informationen 4165
ROSAManageSubscription 4165
Diese Richtlinie wird verwendet 4165
Einzelheiten zur Richtlinie 4165
Version der Richtlinie 4165
JSON-Richtliniendokument 4166
Weitere Informationen 4166

ROSANodePoolManagementPolicy 4167
Diese Richtlinie wird verwendet 4167
Einzelheiten zur Richtlinie 4167
Version der Richtlinie 4167
JSON-Richtliniendokument 4167
Weitere Informationen 4173
ROSASharedVPCEndpointPolicy 4174
Diese Richtlinie wird verwendet 4174
Einzelheiten zur Richtlinie 4174
Version der Richtlinie 4174
JSON-Richtliniendokument 4174
Weitere Informationen 4178
ROSASharedVPCRoute53Policy 4178
Diese Richtlinie wird verwendet 4178
Einzelheiten zur Richtlinie 4179
Version der Richtlinie 4179
JSON-Richtliniendokument 4179
Weitere Informationen 4180
ROSASRESupportPolicy 4180
Diese Richtlinie wird verwendet 4181
Einzelheiten zur Richtlinie 4181
Version der Richtlinie 4181
JSON-Richtliniendokument 4181
Weitere Informationen 4186
ROSAWorkerInstancePolicy 4186
Diese Richtlinie wird verwendet 4186
Einzelheiten zur Richtlinie 4186
Version der Richtlinie 4187
JSON-Richtliniendokument 4187
Weitere Informationen 4188
Route53RecoveryReadinessServiceRolePolicy 4188
Diese Richtlinie wird verwendet 4188
Einzelheiten der Richtlinie 4188
Version der Richtlinie 4189
JSON-Richtliniendokument 4189
Weitere Informationen 4192

Route53ResolverServiceRolePolicy 4192
Diese Richtlinie wird verwendet 4193
Einzelheiten der Richtlinie 4193
Version der Richtlinie 4193
JSON-Richtliniendokument 4193
Weitere Informationen 4194
RTBFabricServiceRolePolicy 4194
Diese Richtlinie wird verwendet 4194
Einzelheiten der Richtlinie 4194
Version der Richtlinie 4194
JSON-Richtliniendokument 4195
Weitere Informationen 4197
S3StorageLensServiceRolePolicy 4197
Diese Richtlinie wird verwendet 4197
Einzelheiten der Richtlinie 4197
Version der Richtlinie 4198
JSON-Richtliniendokument 4198
Weitere Informationen 4198
SageMakerStudioAdminIAMConsolePolicy 4199
Diese Richtlinie wird verwendet 4199
Einzelheiten zur Richtlinie 4199
Version der Richtlinie 4199
JSON-Richtliniendokument 4199
Weitere Informationen 4210
SageMakerStudioAdminIAMDefaultExecutionPolicy 4210
Diese Richtlinie wird verwendet 4210
Einzelheiten zur Richtlinie 4211
Version der Richtlinie 4211
JSON-Richtliniendokument 4211
Weitere Informationen 4232
SageMakerStudioAdminIAMPermissiveExecutionPolicy 4232
Diese Richtlinie wird verwendet 4232
Einzelheiten zur Richtlinie 4233
Version der Richtlinie 4233
JSON-Richtliniendokument 4233
Weitere Informationen 4249

SageMakerStudioAdminProjectUserRolePolicy 4249
Diese Richtlinie wird verwendet 4249
Einzelheiten zur Richtlinie 4249
Version der Richtlinie 4249
JSON-Richtliniendokument 4250
Weitere Informationen 4252
SageMakerStudioBedrockAgentServiceRolePolicy 4252
Diese Richtlinie wird verwendet 4253
Einzelheiten zur Richtlinie 4253
Version der Richtlinie 4253
JSON-Richtliniendokument 4253
Weitere Informationen 4256
SageMakerStudioBedrockChatAgentUserRolePolicy 4257
Diese Richtlinie wird verwendet 4257
Einzelheiten zur Richtlinie 4257
Version der Richtlinie 4257
JSON-Richtliniendokument 4257
Weitere Informationen 4262
SageMakerStudioBedrockEvaluationJobServiceRolePolicy 4262
Diese Richtlinie wird verwendet 4262
Einzelheiten zur Richtlinie 4262
Version der Richtlinie 4262
JSON-Richtliniendokument 4263
Weitere Informationen 4266
SageMakerStudioBedrockFlowServiceRolePolicy 4266
Diese Richtlinie wird verwendet 4267
Einzelheiten zur Richtlinie 4267
Version der Richtlinie 4267
JSON-Richtliniendokument 4267
Weitere Informationen 4271
SageMakerStudioBedrockFunctionExecutionRolePolicy 4271
Diese Richtlinie wird verwendet 4271
Einzelheiten zur Richtlinie 4271
Version der Richtlinie 4272
JSON-Richtliniendokument 4272
Weitere Informationen 4273

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy 4273
Diese Richtlinie wird verwendet 4273
Einzelheiten zur Richtlinie 4273
Version der Richtlinie 4274
JSON-Richtliniendokument 4274
Weitere Informationen 4275
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy 4275
Diese Richtlinie wird verwendet 4275
Einzelheiten zur Richtlinie 4275
Version der Richtlinie 4276
JSON-Richtliniendokument 4276
Weitere Informationen 4281
SageMakerStudioBedrockPromptUserRolePolicy 4282
Diese Richtlinie wird verwendet 4282
Einzelheiten zur Richtlinie 4282
Version der Richtlinie 4282
JSON-Richtliniendokument 4282
Weitere Informationen 4285
SageMakerStudioDomainExecutionRolePolicy 4285
Diese Richtlinie wird verwendet 4285
Einzelheiten zur Richtlinie 4285
Version der Richtlinie 4285
JSON-Richtliniendokument 4286
Weitere Informationen 4292
SageMakerStudioDomainServiceRolePolicy 4292
Diese Richtlinie wird verwendet 4292
Einzelheiten zur Richtlinie 4292
Version der Richtlinie 4293
JSON-Richtliniendokument 4293
Weitere Informationen 4294
SageMakerStudioEMRContainersSystemNamespaceRolePolicy 4294
Diese Richtlinie wird verwendet 4294
Einzelheiten zur Richtlinie 4294
Version der Richtlinie 4295
JSON-Richtliniendokument 4295
Weitere Informationen 4296

SageMakerStudioEMRInstanceRolePolicy 4297
Diese Richtlinie wird verwendet 4297
Einzelheiten zur Richtlinie 4297
Version der Richtlinie 4297
JSON-Richtliniendokument 4297
Weitere Informationen 4301
SageMakerStudioEMRServiceRolePolicy 4301
Diese Richtlinie wird verwendet 4301
Einzelheiten zur Richtlinie 4301
Version der Richtlinie 4302
JSON-Richtliniendokument 4302
Weitere Informationen 4304
SageMakerStudioFullAccess 4304
Diese Richtlinie wird verwendet 4304
Einzelheiten zur Richtlinie 4304
Version der Richtlinie 4305
JSON-Richtliniendokument 4305
Weitere Informationen 4315
SageMakerStudioProjectProvisioningRolePolicy 4315
Diese Richtlinie wird verwendet 4315
Einzelheiten zur Richtlinie 4315
Version der Richtlinie 4316
JSON-Richtliniendokument 4316
Weitere Informationen 4386
SageMakerStudioProjectRoleMachineLearningPolicy 4387
Diese Richtlinie wird verwendet 4387
Einzelheiten zur Richtlinie 4387
Version der Richtlinie 4387
JSON-Richtliniendokument 4387
Weitere Informationen 4413
SageMakerStudioProjectUserRolePermissionsBoundary 4413
Diese Richtlinie wird verwendet 4414
Einzelheiten zur Richtlinie 4414
Version der Richtlinie 4414
JSON-Richtliniendokument 4414
Weitere Informationen 4469

SageMakerStudioProjectUserRolePolicy 4470
Diese Richtlinie wird verwendet 4470
Einzelheiten zur Richtlinie 4470
Version der Richtlinie 4470
JSON-Richtliniendokument 4470
Weitere Informationen 4535
SageMakerStudioQueryExecutionRolePolicy 4536
Diese Richtlinie wird verwendet 4536
Einzelheiten zur Richtlinie 4536
Version der Richtlinie 4536
JSON-Richtliniendokument 4536
Weitere Informationen 4538
SageMakerStudioUserIAMConsolePolicy 4538
Diese Richtlinie wird verwendet 4539
Einzelheiten zur Richtlinie 4539
Version der Richtlinie 4539
JSON-Richtliniendokument 4539
Weitere Informationen 4541
SageMakerStudioUserIAMDefaultExecutionPolicy 4541
Diese Richtlinie wird verwendet 4541
Einzelheiten zur Richtlinie 4541
Version der Richtlinie 4541
JSON-Richtliniendokument 4542
Weitere Informationen 4563
SageMakerStudioUserIAMPermissiveExecutionPolicy 4563
Diese Richtlinie wird verwendet 4564
Einzelheiten zur Richtlinie 4564
Version der Richtlinie 4564
JSON-Richtliniendokument 4564
Weitere Informationen 4578
SecretsManagerReadWrite 4579
Diese Richtlinie wird verwendet 4579
Einzelheiten zur Richtlinie 4579
Version der Richtlinie 4579
JSON-Richtliniendokument 4579
Weitere Informationen 4581

SecurityAgentWebAppAPIPolicy 4581
Diese Richtlinie wird verwendet 4581
Einzelheiten zur Richtlinie 4581
Version der Richtlinie 4582
JSON-Richtliniendokument 4582
Weitere Informationen 4583
SecurityAudit 4584
Diese Richtlinie wird verwendet 4584
Einzelheiten zur Richtlinie 4584
Version der Richtlinie 4584
JSON-Richtliniendokument 4584
Weitere Informationen 4606
SecurityLakeResourceManagementServiceRolePolicy 4606
Diese Richtlinie wird verwendet 4607
Einzelheiten der Richtlinie 4607
Version der Richtlinie 4607
JSON-Richtliniendokument 4607
Weitere Informationen 4613
SecurityLakeServiceLinkedRole 4613
Diese Richtlinie wird verwendet 4613
Einzelheiten der Richtlinie 4613
Version der Richtlinie 4613
JSON-Richtliniendokument 4614
Weitere Informationen 4616
ServerMigration_ServiceRole 4617
Diese Richtlinie wird verwendet 4617
Einzelheiten zur Richtlinie 4617
Version der Richtlinie 4617
JSON-Richtliniendokument 4617
Weitere Informationen 4622
ServerMigrationConnector 4622
Diese Richtlinie wird verwendet 4623
Einzelheiten zur Richtlinie 4623
Version der Richtlinie 4623
JSON-Richtliniendokument 4623
Weitere Informationen 4625

ServerMigrationServiceConsoleFullAccess 4625
Diese Richtlinie wird verwendet 4625
Einzelheiten zur Richtlinie 4625
Version der Richtlinie 4625
JSON-Richtliniendokument 4626
Weitere Informationen 4627
ServerMigrationServiceLaunchRole 4627
Diese Richtlinie wird verwendet 4628
Einzelheiten zur Richtlinie 4628
Version der Richtlinie 4628
JSON-Richtliniendokument 4628
Weitere Informationen 4631
ServerMigrationServiceRoleForInstanceValidation 4631
Diese Richtlinie wird verwendet 4631
Einzelheiten zur Richtlinie 4631
Version der Richtlinie 4632
JSON-Richtliniendokument 4632
Weitere Informationen 4632
ServiceQuotasFullAccess 4632
Diese Richtlinie wird verwendet 4633
Einzelheiten zur Richtlinie 4633
Version der Richtlinie 4633
JSON-Richtliniendokument 4633
Weitere Informationen 4635
ServiceQuotasReadOnlyAccess 4635
Diese Richtlinie wird verwendet 4635
Einzelheiten zur Richtlinie 4635
Version der Richtlinie 4635
JSON-Richtliniendokument 4636
Weitere Informationen 4637
ServiceQuotasServiceRolePolicy 4637
Diese Richtlinie wird verwendet 4637
Einzelheiten der Richtlinie 4638
Version der Richtlinie 4638
JSON-Richtliniendokument 4638
Weitere Informationen 4638

SignInLocalDevelopmentAccess 4639
Diese Richtlinie wird verwendet 4639
Einzelheiten zur Richtlinie 4639
Version der Richtlinie 4639
JSON-Richtliniendokument 4639
Weitere Informationen 4640
SimpleWorkflowFullAccess 4640
Diese Richtlinie wird verwendet 4640
Einzelheiten zur Richtlinie 4640
Version der Richtlinie 4640
JSON-Richtliniendokument 4641
Weitere Informationen 4641
SMSVoiceServiceRolePolicy 4641
Diese Richtlinie wird verwendet 4641
Einzelheiten der Richtlinie 4641
Version der Richtlinie 4642
JSON-Richtliniendokument 4642
Weitere Informationen 4642
SplitCostAllocationDataServiceRolePolicy 4643
Diese Richtlinie wird verwendet 4643
Einzelheiten der Richtlinie 4643
Version der Richtlinie 4643
JSON-Richtliniendokument 4643
Weitere Informationen 4644
SSMQuickSetupRolePolicy 4644
Diese Richtlinie wird verwendet 4644
Einzelheiten der Richtlinie 4645
Version der Richtlinie 4645
JSON-Richtliniendokument 4645
Weitere Informationen 4648
SupportUser 4648
Diese Richtlinie wird verwendet 4648
Einzelheiten zur Richtlinie 4648
Version der Richtlinie 4649
JSON-Richtliniendokument 4649
Weitere Informationen 4654

SystemAdministrator 4654
Diese Richtlinie wird verwendet 4654
Einzelheiten zur Richtlinie 4654
Version der Richtlinie 4655
JSON-Richtliniendokument 4655
Weitere Informationen 4661
TranslateFullAccess 4661
Diese Richtlinie wird verwendet 4661
Einzelheiten zur Richtlinie 4661
Version der Richtlinie 4662
JSON-Richtliniendokument 4662
Weitere Informationen 4662
TranslateReadOnly 4663
Diese Richtlinie wird verwendet 4663
Einzelheiten zur Richtlinie 4663
Version der Richtlinie 4663
JSON-Richtliniendokument 4663
Weitere Informationen 4664
ViewOnlyAccess 4664
Diese Richtlinie wird verwendet 4664
Einzelheiten zur Richtlinie 4664
Version der Richtlinie 4665
JSON-Richtliniendokument 4665
Weitere Informationen 4674
VMImportExportRoleForAWSConnector 4674
Diese Richtlinie wird verwendet 4674
Einzelheiten zur Richtlinie 4675
Version der Richtlinie 4675
JSON-Richtliniendokument 4675
Weitere Informationen 4676
VPCLatticeFullAccess 4676
Diese Richtlinie wird verwendet 4676
Einzelheiten zur Richtlinie 4676
Version der Richtlinie 4676
JSON-Richtliniendokument 4677
Weitere Informationen 4679

VPCLatticeReadOnlyAccess 4679
Diese Richtlinie wird verwendet 4679
Einzelheiten zur Richtlinie 4679
Version der Richtlinie 4679
JSON-Richtliniendokument 4680
Weitere Informationen 4680
VPCLatticeServicesInvokeAccess 4681
Diese Richtlinie wird verwendet 4681
Einzelheiten zur Richtlinie 4681
Version der Richtlinie 4681
JSON-Richtliniendokument 4681
Weitere Informationen 4682
WAFLoggingServiceRolePolicy 4682
Diese Richtlinie wird verwendet 4682
Einzelheiten der Richtlinie 4682
Version der Richtlinie 4682
JSON-Richtliniendokument 4683
Weitere Informationen 4683
WAFRegionalLoggingServiceRolePolicy 4683
Diese Richtlinie wird verwendet 4683
Einzelheiten der Richtlinie 4684
Version der Richtlinie 4684
JSON-Richtliniendokument 4684
Weitere Informationen 4684
WAFV2LoggingServiceRolePolicy 4685
Diese Richtlinie wird verwendet 4685
Einzelheiten der Richtlinie 4685
Version der Richtlinie 4685
JSON-Richtliniendokument 4685
Weitere Informationen 4686
WellArchitectedConsoleFullAccess 4686
Diese Richtlinie wird verwendet 4686
Einzelheiten zur Richtlinie 4686
Version der Richtlinie 4687
JSON-Richtliniendokument 4687
Weitere Informationen 4687

WellArchitectedConsoleReadOnlyAccess 4688
Diese Richtlinie wird verwendet 4688
Einzelheiten zur Richtlinie 4688
Version der Richtlinie 4688
JSON-Richtliniendokument 4688
Weitere Informationen 4689
WorkLinkServiceRolePolicy 4689
Diese Richtlinie wird verwendet 4689
Einzelheiten zur Richtlinie 4689
Version der Richtlinie 4689
JSON-Richtliniendokument 4690
Weitere Informationen 4690
..... mmmmdcxci

Was sind AWS verwaltete Richtlinien?

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen. Sie erleichtern Ihnen den Einstieg in die Zuweisung von Berechtigungen an Benutzer, Gruppen und Rollen, als wenn Sie die Richtlinien selbst schreiben müssten.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie von allen Kunden verwendet werden können. AWS Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn ein neuer AWS Dienst gestartet wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Referenzseiten zu Richtlinien verstehen

Jede Referenzseite für Richtlinien enthält die folgenden Informationen:

- Verwendung dieser Richtlinie — Gibt an, ob Sie die Richtlinie Benutzern, Gruppen und Rollen zuordnen können
- Einzelheiten der Richtlinie
  - Typ — Der Typ der AWS verwalteten Richtlinie
    - `AWS managed policy`— Eine AWS verwaltete Standardrichtlinie
    - `Job function policy`— Eine Politik, die sich an den üblichen beruflichen Funktionen der Branche orientiert
    - `Service-linked role policy`— Richtlinie, die mit einer dienstbezogenen Rolle verknüpft ist und es einem Dienst ermöglicht, in Ihrem Namen Aktionen durchzuführen, wie z. B. the section called “AmazonRDSPreviewServiceRolePolicy”
    - `Service role policy`— Richtlinie, die für die Arbeit mit Servicerollen konzipiert ist, wie z. B. the section called “AWSControlTowerServiceRolePolicy”

  - Erstellungszeit — Wann die Richtlinie zum ersten Mal erstellt wurde
  - Zeitpunkt der Bearbeitung — Wann diese Version der Richtlinie bearbeitet wurde
  - ARN — Der Amazon-Ressourcenname der Richtlinie
- Richtlinienversion — Die Version der durch die Richtlinie gewährten Berechtigungen
- JSON-Richtliniendokument — Das Richtlinien-JSON
- Weitere Informationen — Links zur Dokumentation zu AWS verwalteten Richtlinien

Veraltete verwaltete Richtlinien AWS

AWS aktualisiert regelmäßig AWS verwaltete Richtlinien. In den meisten Fällen fügen wir einer Richtlinie Berechtigungen hinzu. Dies passiert, wenn wir einen neuen Dienst oder eine neue Funktion starten. Um die Sicherheit AWS verwalteter Richtlinien zu verbessern, reduzieren wir manchmal den Geltungsbereich der Richtlinien. Wenn wir Berechtigungen aus einer Richtlinie entfernen, setzen wir die Richtlinie auf den Status „Veraltet“ und stellen eine neue Richtlinie zur Verfügung. Wenn ein Dienst oder eine AWS Funktion als veraltet eingestuft wird, gilt auch die verwaltete Richtlinie für diese Funktion als veraltet. AWS

Wenn Sie eine E-Mail-Benachrichtigung erhalten, dass eine von Ihnen verwendete Richtlinie veraltet ist, empfehlen wir Ihnen, sofort Maßnahmen zu ergreifen. Identifizieren Sie die Änderung an der Richtlinie und aktualisieren Sie Ihre Workflows. Wenn AWS eine Ersatzrichtlinie bereitgestellt wird, planen Sie, diese allen betroffenen Identitäten (Benutzern, Gruppen und Rollen) zuzuordnen und dann die veraltete Richtlinie von diesen Identitäten zu trennen.

Eine veraltete Richtlinie hat folgende Merkmale:

- Sie wurde aus diesem Handbuch entfernt.
- Die Berechtigungen funktionieren weiterhin für alle derzeit angehängten Identitäten.
- In Konten, bei denen die Richtlinie an eine Identität angehängt ist, wird sie in der Richtlinienliste der IAM-Konsole mit einem Warnsymbol daneben angezeigt.
- Sie kann nicht an neue Identitäten angehängt werden. Wenn Sie es von einer aktuellen Identität trennen, können Sie es nicht erneut anhängen.
- Nachdem Sie es von allen aktuellen Entitäten getrennt haben, ist es nicht mehr sichtbar.

AWS verwaltete Richtlinien

AWS verwaltete Richtlinien

- AccessAnalyzerServiceRolePolicy
- AccountManagementFromVercel
- AdministratorAccess
- AdministratorAccess-Amplify
- AdministratorAccess-AWSElasticBeanstalk
- AIOpsAssistantIncidentReportPolicy
- AIOpsAssistantPolicy
- AIOpsConsoleAdminPolicy
- AIOpsOperatorAccess
- AIOpsReadOnlyAccess
- AlexaForBusinessDeviceSetup
- AlexaForBusinessFullAccess
- AlexaForBusinessGatewayExecution
- AlexaForBusinessLifesizeDelegatedAccessPolicy
- AlexaForBusinessNetworkProfileServicePolicy
- AlexaForBusinessPolyDelegatedAccessPolicy
- AlexaForBusinessReadOnlyAccess
- AmazonAPIGatewayAdministrator
- AmazonAPIGatewayInvokeFullAccess
- AmazonAPIGatewayPushToCloudWatchLogs
- AmazonAppFlowFullAccess
- AmazonAppFlowReadOnlyAccess
- AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy
- AmazonAppStreamFullAccess
- AmazonAppStreamPCAAccess
- AmazonAppStreamReadOnlyAccess

- AmazonAppStreamServiceAccess
- AmazonAthenaFullAccess
- AmazonAthenaServiceRolePolicy
- AmazonAugmentedAIFullAccess
- AmazonAugmentedAIHumanLoopFullAccess
- AmazonAugmentedAIIntegratedAPIAccess
- AmazonAuroraDSQLConsoleFullAccess
- AmazonAuroraDSQLFullAccess
- AmazonAuroraDSQLReadOnlyAccess
- AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy
- AmazonBedrockFullAccess
- AmazonBedrockLimitedAccess
- AmazonBedrockMantleFullAccess
- AmazonBedrockMantleInferenceAccess
- AmazonBedrockMantleReadOnly
- AmazonBedrockMarketplaceAccess
- AmazonBedrockReadOnly
- AmazonBedrockStudioPermissionsBoundary
- AmazonBraketFullAccess
- AmazonBraketJobsExecutionPolicy
- AmazonBraketServiceRolePolicy
- AmazonChimeFullAccess
- AmazonChimeReadOnly
- AmazonChimeSDK
- AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy
- AmazonChimeSDKMessagingServiceRolePolicy
- AmazonChimeServiceRolePolicy
- AmazonChimeTranscriptionServiceLinkedRolePolicy
- AmazonChimeUserManagement

- AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- AmazonCloudDirectoryFullAccess
- AmazonCloudDirectoryReadOnlyAccess
- AmazonCloudWatchEvidentlyFullAccess
- AmazonCloudWatchEvidentlyReadOnlyAccess
- AmazonCloudWatchEvidentlyServiceRolePolicy
- AmazonCloudWatchRUMFullAccess
- AmazonCloudWatchRUMReadOnlyAccess
- AmazonCloudWatchRUMServiceRolePolicy
- AmazonCodeCatalystFullAccess
- AmazonCodeCatalystReadOnlyAccess
- AmazonCodeCatalystSupportAccess
- AmazonCodeGuruProfilerAgentAccess
- AmazonCodeGuruProfilerFullAccess
- AmazonCodeGuruProfilerReadOnlyAccess
- AmazonCodeGuruReviewerFullAccess
- AmazonCodeGuruReviewerReadOnlyAccess
- AmazonCodeGuruReviewerServiceRolePolicy
- AmazonCodeGuruSecurityFullAccess
- AmazonCodeGuruSecurityScanAccess
- AmazonCognitoDeveloperAuthenticatedIdentities
- AmazonCognitoIdpEmailServiceRolePolicy
- AmazonCognitoIdpServiceRolePolicy
- AmazonCognitoPowerUser
- AmazonCognitoReadOnly
- AmazonCognitoUnAuthedIdentitiesSessionPolicy
- AmazonCognitoUnauthenticatedIdentities
- AmazonConnect_FullAccess
- AmazonConnectCampaignsServiceLinkedRolePolicy

- AmazonConnectReadOnlyAccess
- AmazonConnectServiceLinkedRolePolicy
- AmazonConnectSynchronizationServiceRolePolicy
- AmazonConnectVoiceIDFullAccess
- AmazonDataZoneBedrockModelConsumptionPolicy
- AmazonDataZoneBedrockModelManagementPolicy
- AmazonDataZoneDomainExecutionRolePolicy
- AmazonDataZoneEnvironmentRolePermissionsBoundary
- AmazonDataZoneFullAccess
- AmazonDataZoneFullUserAccess
- AmazonDataZoneGlueManageAccessRolePolicy
- AmazonDataZonePortalFullAccessPolicy
- AmazonDataZonePreviewConsoleFullAccess
- AmazonDataZoneProjectDeploymentPermissionsBoundary
- AmazonDataZoneProjectRolePermissionsBoundary
- AmazonDataZoneRedshiftGlueProvisioningPolicy
- AmazonDataZoneRedshiftManageAccessRolePolicy
- AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- AmazonDataZoneSageMakerManageAccessRolePolicy
- AmazonDataZoneSageMakerProvisioningRolePolicy
- AmazonDetectiveFullAccess
- AmazonDetectiveInvestigatorAccess
- AmazonDetectiveMemberAccess
- AmazonDetectiveOrganizationsAccess
- AmazonDetectiveServiceLinkedRolePolicy
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruOrganizationsAccess
- AmazonDevOpsGuruReadOnlyAccess

- AmazonDevOpsGuruServiceRolePolicy
- AmazonDMSCloudWatchLogsRole
- AmazonDMSRedshiftS3Role
- AmazonDMSVPCManagementRole
- AmazonDocDB-ElasticServiceRolePolicy
- AmazonDocDBConsoleFullAccess
- AmazonDocDBElasticFullAccess
- AmazonDocDBElasticReadOnlyAccess
- AmazonDocDBFullAccess
- AmazonDocDBReadOnlyAccess
- AmazonDRSVPCManagement
- AmazonDynamoDBFullAccess
- AmazonDynamoDBFullAccess_v2
- AmazonDynamoDBFullAccesswithDataPipeline
- AmazonDynamoDBReadOnlyAccess
- AmazonEBSCSIDriverPolicy
- AmazonEC2ContainerRegistryFullAccess
- AmazonEC2ContainerRegistryPowerUser
- AmazonEC2ContainerRegistryPullOnly
- AmazonEC2ContainerRegistryReadOnly
- AmazonEC2ContainerServiceAutoscaleRole
- AmazonEC2ContainerServiceEventsRole
- AmazonEC2ContainerServiceforEC2Role
- AmazonEC2ContainerServiceRole
- AmazonEC2FullAccess
- AmazonEC2ImageReferencesAccessPolicy
- AmazonEC2ReadOnlyAccess
- AmazonEC2RoleforAWSCodeDeploy
- AmazonEC2RoleforAWSCodeDeployLimited

- AmazonEC2RoleforDataPipelineRole
- AmazonEC2RoleforSSM
- AmazonEC2RolePolicyForLaunchWizard
- AmazonEC2SpotFleetAutoscaleRole
- AmazonEC2SpotFleetTaggingRole
- AmazonECS_FullAccess
- AmazonECSComputeServiceRolePolicy
- AmazonECSInfrastructureRoleforExpressGatewayServices
- AmazonECSInfrastructureRolePolicyForLoadBalancers
- AmazonECSInfrastructureRolePolicyForManagedInstances
- AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
- AmazonECSInfrastructureRolePolicyForVolumes
- AmazonECSInfrastructureRolePolicyForVpcLattice
- AmazonECSInstanceRolePolicyForManagedInstances
- AmazonECSServiceRolePolicy
- AmazonECSTaskExecutionRolePolicy
- AmazonEFSCSIDriverPolicy
- AmazonEKS_CNI_Policy
- AmazonEKSBlockStoragePolicy
- AmazonEKSClusterPolicy
- AmazonEKSComputePolicy
- AmazonEKSConnectorServiceRolePolicy
- AmazonEKSDashboardConsoleReadOnly
- AmazonEKSDashboardServiceRolePolicy
- AmazonEKSFargatePodExecutionRolePolicy
- AmazonEKSForFargateServiceRolePolicy
- AmazonEKSLoadBalancingPolicy
- AmazonEKSLocalOutpostClusterPolicy
- AmazonEKSLocalOutpostServiceRolePolicy

- AmazonEKSMCPReadOnlyAccess
- AmazonEKSNetworkingPolicy
- AmazonEKSServicePolicy
- AmazonEKSServiceRolePolicy
- AmazonEKSVPCResourceController
- AmazonEKSWorkerNodeMinimalPolicy
- AmazonEKSWorkerNodePolicy
- AmazonElastiCacheFullAccess
- AmazonElastiCacheReadOnlyAccess
- AmazonElasticContainerRegistryPublicFullAccess
- AmazonElasticContainerRegistryPublicPowerUser
- AmazonElasticContainerRegistryPublicReadOnly
- AmazonElasticFileSystemClientFullAccess
- AmazonElasticFileSystemClientReadOnlyAccess
- AmazonElasticFileSystemClientReadWriteAccess
- AmazonElasticFileSystemFullAccess
- AmazonElasticFileSystemReadOnlyAccess
- AmazonElasticFileSystemServiceRolePolicy
- AmazonElasticFileSystemsUtils
- AmazonElasticMapReduceEditorsRole
- AmazonElasticMapReduceforAutoScalingRole
- AmazonElasticMapReduceforEC2Role
- AmazonElasticMapReduceFullAccess
- AmazonElasticMapReducePlacementGroupPolicy
- AmazonElasticMapReduceReadOnlyAccess
- AmazonElasticMapReduceRole
- AmazonElasticsearchServiceRolePolicy
- AmazonElasticTranscoder_FullAccess
- AmazonElasticTranscoder_JobsSubmitter

- AmazonElasticTranscoder_ReadOnlyAccess
- AmazonElasticTranscoderRole
- AmazonEMRCleanupPolicy
- AmazonEMRContainersServiceRolePolicy
- AmazonEMRFullAccessPolicy_v2
- AmazonEMRReadOnlyAccessPolicy_v2
- AmazonEMRServerlessServiceRolePolicy
- AmazonEMRServicePolicy_v2
- AmazonESCognitoAccess
- AmazonESFullAccess
- AmazonESReadOnlyAccess
- AmazonEventBridgeApiDestinationsServiceRolePolicy
- AmazonEventBridgeFullAccess
- AmazonEventBridgePipesFullAccess
- AmazonEventBridgePipesOperatorAccess
- AmazonEventBridgePipesReadOnlyAccess
- AmazonEventBridgeReadOnlyAccess
- AmazonEventBridgeSchedulerFullAccess
- AmazonEventBridgeSchedulerReadOnlyAccess
- AmazonEventBridgeSchemasFullAccess
- AmazonEventBridgeSchemasReadOnlyAccess
- AmazonEventBridgeSchemasServiceRolePolicy
- AmazonEVSServiceRolePolicy
- AmazonFISServiceRolePolicy
- AmazonForecastFullAccess
- AmazonFraudDetectorFullAccessPolicy
- AmazonFreeRTOSFullAccess
- AmazonFreeRTOSOTAUpdate
- AmazonFSxConsoleFullAccess

- AmazonFSxConsoleReadOnlyAccess
- AmazonFSxFullAccess
- AmazonFSxReadOnlyAccess
- AmazonFSxServiceRolePolicy
- AmazonGlacierFullAccess
- AmazonGlacierReadOnlyAccess
- AmazonGrafanaAthenaAccess
- AmazonGrafanaCloudWatchAccess
- AmazonGrafanaRedshiftAccess
- AmazonGrafanaServiceLinkedRolePolicy
- AmazonGuardDutyFullAccess
- AmazonGuardDutyFullAccess_v2
- AmazonGuardDutyMalwareProtectionServiceRolePolicy
- AmazonGuardDutyReadOnlyAccess
- AmazonGuardDutyServiceRolePolicy
- AmazonHealthLakeFullAccess
- AmazonHealthLakeReadOnlyAccess
- AmazonHoneycodeFullAccess
- AmazonHoneycodeReadOnlyAccess
- AmazonHoneycodeServiceRolePolicy
- AmazonHoneycodeTeamAssociationFullAccess
- AmazonHoneycodeTeamAssociationReadOnlyAccess
- AmazonHoneycodeWorkbookFullAccess
- AmazonHoneycodeWorkbookReadOnlyAccess
- AmazonInspector2AgentlessServiceRolePolicy
- AmazonInspector2FullAccess
- AmazonInspector2FullAccess_v2
- AmazonInspector2ManagedCisPolicy
- AmazonInspector2ReadOnlyAccess

- AmazonInspector2ServiceRolePolicy
- AmazonInspectorFullAccess
- AmazonInspectorReadOnlyAccess
- AmazonInspectorServiceRolePolicy
- AmazonKendraFullAccess
- AmazonKendraReadOnlyAccess
- AmazonKeyspacesFullAccess
- AmazonKeyspacesReadOnlyAccess
- AmazonKeyspacesReadOnlyAccess_v2
- AmazonKinesisAnalyticsFullAccess
- AmazonKinesisAnalyticsReadOnly
- AmazonKinesisFirehoseFullAccess
- AmazonKinesisFirehoseReadOnlyAccess
- AmazonKinesisFullAccess
- AmazonKinesisReadOnlyAccess
- AmazonKinesisVideoStreamsFullAccess
- AmazonKinesisVideoStreamsReadOnlyAccess
- AmazonLaunchWizard_Fullaccess
- AmazonLaunchWizardFullAccessV2
- AmazonLexChannelsAccess
- AmazonLexFullAccess
- AmazonLexReadOnly
- AmazonLexReplicationPolicy
- AmazonLexRunBotsOnly
- AmazonLexV2BotPolicy
- AmazonLookoutEquipmentFullAccess
- AmazonLookoutEquipmentReadOnlyAccess
- AmazonLookoutMetricsFullAccess
- AmazonLookoutMetricsReadOnlyAccess

- AmazonLookoutVisionConsoleFullAccess
- AmazonLookoutVisionConsoleReadOnlyAccess
- AmazonLookoutVisionFullAccess
- AmazonLookoutVisionReadOnlyAccess
- AmazonMachineLearningBatchPredictionsAccess
- AmazonMachineLearningCreateOnlyAccess
- AmazonMachineLearningFullAccess
- AmazonMachineLearningManageRealTimeEndpointOnlyAccess
- AmazonMachineLearningReadOnlyAccess
- AmazonMachineLearningRealTimePredictionOnlyAccess
- AmazonMachineLearningRoleforRedshiftDataSourceV3
- AmazonMacieFullAccess
- AmazonMacieHandshakeRole
- AmazonMacieReadOnlyAccess
- AmazonMacieServiceRole
- AmazonMacieServiceRolePolicy
- AmazonManagedBlockchainConsoleFullAccess
- AmazonManagedBlockchainFullAccess
- AmazonManagedBlockchainReadOnlyAccess
- AmazonManagedBlockchainServiceRolePolicy
- AmazonMCSFullAccess
- AmazonMCSReadOnlyAccess
- AmazonMechanicalTurkFullAccess
- AmazonMechanicalTurkReadOnly
- AmazonMemoryDBFullAccess
- AmazonMemoryDBReadOnlyAccess
- AmazonMobileAnalyticsFinancialReportAccess
- AmazonMobileAnalyticsFullAccess
- AmazonMobileAnalyticsNon-financialReportAccess

- AmazonMobileAnalyticsWriteOnlyAccess
- AmazonMonitronFullAccess
- AmazonMQApiFullAccess
- AmazonMQApiReadOnlyAccess
- AmazonMQFullAccess
- AmazonMQReadOnlyAccess
- AmazonMQServiceRolePolicy
- AmazonMSKConnectReadOnlyAccess
- AmazonMSKFullAccess
- AmazonMSKReadOnlyAccess
- AmazonMWAAServerlessServiceRolePolicy
- AmazonMWAAServiceRolePolicy
- AmazonNimbleStudio-LaunchProfileWorker
- AmazonNimbleStudio-StudioAdmin
- AmazonNimbleStudio-StudioUser
- AmazonODBServiceRolePolicy
- AmazonOmicsFullAccess
- AmazonOmicsReadOnlyAccess
- AmazonOneEnterpriseFullAccess
- AmazonOneEnterpriseInstallerAccess
- AmazonOneEnterpriseReadOnlyAccess
- AmazonOpenSearchDashboardsServiceRolePolicy
- AmazonOpenSearchDirectQueryGlueCreateAccess
- AmazonOpenSearchIngestionFullAccess
- AmazonOpenSearchIngestionReadOnlyAccess
- AmazonOpenSearchIngestionServiceRolePolicy
- AmazonOpenSearchServerlessServiceRolePolicy
- AmazonOpenSearchServiceCognitoAccess
- AmazonOpenSearchServiceFullAccess

- AmazonOpenSearchServiceReadOnlyAccess
- AmazonOpenSearchServiceRolePolicy
- AmazonPersonalizeFullAccess
- AmazonPollyFullAccess
- AmazonPollyReadOnlyAccess
- AmazonPrometheusConsoleFullAccess
- AmazonPrometheusFullAccess
- AmazonPrometheusQueryAccess
- AmazonPrometheusRemoteWriteAccess
- AmazonPrometheusScraperServiceRolePolicy
- AmazonQDeveloperAccess
- AmazonQFullAccess
- AmazonQLDBConsoleFullAccess
- AmazonQLDBFullAccess
- AmazonQLDBReadOnly
- AmazonRDSBetaServiceRolePolicy
- AmazonRDSCustomInstanceProfileRolePolicy
- AmazonRDSCustomPreviewServiceRolePolicy
- AmazonRDSCustomServiceRolePolicy
- AmazonRDSDataFullAccess
- AmazonRDSDirectoryServiceAccess
- AmazonRDSEnhancedMonitoringRole
- AmazonRDSFullAccess
- AmazonRDSPerformanceInsightsFullAccess
- AmazonRDSPerformanceInsightsReadOnly
- AmazonRDSPreviewServiceRolePolicy
- AmazonRDSReadOnlyAccess
- AmazonRDSServiceRolePolicy
- AmazonRedshiftAllCommandsFullAccess

- AmazonRedshiftDataFullAccess
- AmazonRedshiftFederatedAuthorization
- AmazonRedshiftFullAccess
- AmazonRedshiftQueryEditor
- AmazonRedshiftQueryEditorV2FullAccess
- AmazonRedshiftQueryEditorV2NoSharing
- AmazonRedshiftQueryEditorV2ReadSharing
- AmazonRedshiftQueryEditorV2ReadWriteSharing
- AmazonRedshiftReadOnlyAccess
- AmazonRedshiftServiceLinkedRolePolicy
- AmazonRekognitionCustomLabelsFullAccess
- AmazonRekognitionFullAccess
- AmazonRekognitionReadOnlyAccess
- AmazonRekognitionServiceRole
- AmazonRoute53AutoNamingFullAccess
- AmazonRoute53AutoNamingReadOnlyAccess
- AmazonRoute53AutoNamingRegistrantAccess
- AmazonRoute53DomainsFullAccess
- AmazonRoute53DomainsReadOnlyAccess
- AmazonRoute53FullAccess
- AmazonRoute53ProfilesFullAccess
- AmazonRoute53ProfilesReadOnlyAccess
- AmazonRoute53ReadOnlyAccess
- AmazonRoute53RecoveryClusterFullAccess
- AmazonRoute53RecoveryClusterReadOnlyAccess
- AmazonRoute53RecoveryControlConfigFullAccess
- AmazonRoute53RecoveryControlConfigReadOnlyAccess
- AmazonRoute53RecoveryReadinessFullAccess
- AmazonRoute53RecoveryReadinessReadOnlyAccess

- AmazonRoute53ResolverFullAccess
- AmazonRoute53ResolverReadOnlyAccess
- AmazonS3FullAccess
- AmazonS3ObjectLambdaExecutionRolePolicy
- AmazonS3OutpostsFullAccess
- AmazonS3OutpostsReadOnlyAccess
- AmazonS3ReadOnlyAccess
- AmazonS3TablesFullAccess
- AmazonS3TablesLakeFormationServiceRole
- AmazonS3TablesReadOnlyAccess
- AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy
- AmazonSageMakerCanvasAIServicesAccess
- AmazonSageMakerCanvasBedrockAccess
- AmazonSageMakerCanvasDataPrepFullAccess
- AmazonSageMakerCanvasDirectDeployAccess
- AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy
- AmazonSageMakerCanvasForecastAccess
- AmazonSageMakerCanvasFullAccess
- AmazonSageMakerCanvasSMDataScienceAssistantAccess
- AmazonSageMakerClusterInstanceRolePolicy
- AmazonSageMakerCoreServiceRolePolicy
- AmazonSageMakerEdgeDeviceFleetPolicy
- AmazonSageMakerFeatureStoreAccess
- AmazonSageMakerFullAccess
- AmazonSageMakerGeospatialExecutionRole
- AmazonSageMakerGeospatialFullAccess
- AmazonSageMakerGroundTruthExecution
- AmazonSageMakerHyperPodObservabilityAdminAccess
- AmazonSageMakerHyperPodServiceRolePolicy

- AmazonSageMakerHyperPodTrainingOperatorAccess
- AmazonSageMakerMechanicalTurkAccess
- AmazonSageMakerModelGovernanceUseAccess
- AmazonSageMakerModelRegistryFullAccess
- AmazonSageMakerNotebooksServiceRolePolicy
- AmazonSageMakerPartnerAppsFullAccess
- AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy
- AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerPipelinesIntegrations
- AmazonSageMakerQuickSightVPCPolicy
- AmazonSageMakerReadOnly
- AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy
- AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy
- AmazonSageMakerSpacesControllerPolicy
- AmazonSageMakerSpacesRouterPolicy
- AmazonSageMakerTrainingPlanCreateAccess
- AmazonSecurityLakeAdministrator
- AmazonSecurityLakeMetastoreManager
- AmazonSecurityLakePermissionsBoundary
- AmazonSESFullAccess
- AmazonSESReadOnlyAccess
- AmazonSESServiceRolePolicy

- AmazonSNSFullAccess
- AmazonSNSReadOnlyAccess
- AmazonSNSRole
- AmazonSQSFullAccess
- AmazonSQSReadOnlyAccess
- AmazonSSMAutomationApproverAccess
- AmazonSSMAutomationRole
- AmazonSSMDirectoryServiceAccess
- AmazonSSMFullAccess
- AmazonSSMMaintenanceWindowRole
- AmazonSSMManagedEC2InstanceDefaultPolicy
- AmazonSSMManagedInstanceCore
- AmazonSSMPatchAssociation
- AmazonSSMReadOnlyAccess
- AmazonSSMServiceRolePolicy
- AmazonSumerianFullAccess
- AmazonTextractFullAccess
- AmazonTextractServiceRole
- AmazonTimestreamConsoleFullAccess
- AmazonTimestreamFullAccess
- AmazonTimestreamInfluxDBFullAccess
- AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess
- AmazonTimestreamInfluxDBServiceRolePolicy
- AmazonTimestreamReadOnlyAccess
- AmazonTranscribeFullAccess
- AmazonTranscribeReadOnlyAccess
- AmazonVerifiedPermissionsFullAccess
- AmazonVerifiedPermissionsReadOnlyAccess
- AmazonVPCCrossAccountNetworkInterfaceOperations

- AmazonVPCFullAccess
- AmazonVPCNetworkAccessAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerFullAccessPolicy
- AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
- AmazonVPCReadOnlyAccess
- AmazonWorkDocsFullAccess
- AmazonWorkDocsReadOnlyAccess
- AmazonWorkMailEventsServiceRolePolicy
- AmazonWorkMailFullAccess
- AmazonWorkMailMessageFlowFullAccess
- AmazonWorkMailMessageFlowReadOnlyAccess
- AmazonWorkMailReadOnlyAccess
- AmazonWorkSpacesAdmin
- AmazonWorkSpacesApplicationManagerAdminAccess
- AmazonWorkspacesPCAAccess
- AmazonWorkSpacesPoolServiceAccess
- AmazonWorkSpacesSecureBrowserReadOnly
- AmazonWorkSpacesSelfServiceAccess
- AmazonWorkSpacesServiceAccess
- AmazonWorkSpacesThinClientFullAccess
- AmazonWorkSpacesThinClientMonitoringServiceRolePolicy
- AmazonWorkSpacesThinClientReadOnlyAccess
- AmazonWorkSpacesWebReadOnly
- AmazonWorkSpacesWebServiceRolePolicy
- AmazonZocaloFullAccess
- AmazonZocaloReadOnlyAccess
- AmplifyBackendDeployFullAccess
- APIGatewayServiceRolePolicy
- AppIntegrationsServiceLinkedRolePolicy

- ApplicationAutoScalingForAmazonAppStreamAccess
- ApplicationDiscoveryServiceContinuousExportServiceRolePolicy
- AppRunnerNetworkingServiceRolePolicy
- AppRunnerServiceRolePolicy
- AppStudioServiceRolePolicy
- AuroraDsqlServiceLinkedRolePolicy
- AutoScalingConsoleFullAccess
- AutoScalingConsoleReadOnlyAccess
- AutoScalingFullAccess
- AutoScalingNotificationAccessRole
- AutoScalingReadOnlyAccess
- AutoScalingServiceRolePolicy
- AWS-SSM-Automation-DiagnosisBucketPolicy
- AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy
- AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy
- AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy
- AWS-SSM-RemediationAutomation-AdministrationRolePolicy
- AWS-SSM-RemediationAutomation-ExecutionRolePolicy
- AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy
- AWS_ConfigRole
- AWSAccountActivityAccess
- AWSAccountManagementFullAccess
- AWSAccountManagementReadOnlyAccess
- AWSAccountSettingsManagementRole
- AWSAccountUsageReportAccess
- AWSAgentlessDiscoveryService
- AWSAppFabricFullAccess
- AWSAppFabricReadOnlyAccess
- AWSAppFabricServiceRolePolicy

- AWSApplicationAutoscalingAppStreamFleetPolicy
- AWSApplicationAutoscalingCassandraTablePolicy
- AWSApplicationAutoscalingComprehendEndpointPolicy
- AWSApplicationAutoScalingCustomResourcePolicy
- AWSApplicationAutoscalingDynamoDBTablePolicy
- AWSApplicationAutoscalingEC2SpotFleetRequestPolicy
- AWSApplicationAutoscalingECSServicePolicy
- AWSApplicationAutoscalingElastiCacheRGPolicy
- AWSApplicationAutoscalingEMRInstanceGroupPolicy
- AWSApplicationAutoscalingKafkaClusterPolicy
- AWSApplicationAutoscalingLambdaConcurrencyPolicy
- AWSApplicationAutoscalingNeptuneClusterPolicy
- AWSApplicationAutoscalingRDSClusterPolicy
- AWSApplicationAutoscalingSageMakerEndpointPolicy
- AWSApplicationAutoscalingWorkSpacesPoolPolicy
- AWSApplicationDiscoveryAgentAccess
- AWSApplicationDiscoveryAgentlessCollectorAccess
- AWSApplicationDiscoveryServiceFullAccess
- AWSApplicationMigrationAgentInstallationPolicy
- AWSApplicationMigrationAgentPolicy
- AWSApplicationMigrationAgentPolicy_v2
- AWSApplicationMigrationConversionServerPolicy
- AWSApplicationMigrationEC2Access
- AWSApplicationMigrationFullAccess
- AWSApplicationMigrationMGHAccess
- AWSApplicationMigrationNetworkMigrationCustomResource
- AWSApplicationMigrationNetworkMigrationMultiAccount
- AWSApplicationMigrationReadOnlyAccess
- AWSApplicationMigrationReplicationServerPolicy

- AWSApplicationMigrationServiceEc2InstancePolicy
- AWSApplicationMigrationServiceRolePolicy
- AWSApplicationMigrationSSMAccess
- AWSApplicationMigrationVCenterClientPolicy
- AWSAppMeshEnvoyAccess
- AWSAppMeshFullAccess
- AWSAppMeshPreviewEnvoyAccess
- AWSAppMeshPreviewServiceRolePolicy
- AWSAppMeshReadOnly
- AWSAppMeshServiceRolePolicy
- AWSAppRunnerFullAccess
- AWSAppRunnerReadOnlyAccess
- AWSAppRunnerServicePolicyForECRAccess
- AWSAppSyncAdministrator
- AWSAppSyncInvokeFullAccess
- AWSAppSyncPushToCloudWatchLogs
- AWSAppSyncSchemaAuthor
- AWSAppSyncServiceRolePolicy
- AWSArtifactAccountSync
- AWSArtifactAgreementsFullAccess
- AWSArtifactAgreementsReadOnlyAccess
- AWSArtifactReportsReadOnlyAccess
- AWSArtifactServiceRolePolicy
- AWSAuditManagerAdministratorAccess
- AWSAuditManagerServiceRolePolicy
- AWSAutoScalingPlansEC2AutoScalingPolicy
- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess

- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupGuardDutyRolePolicyForScans
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupSearchOperatorAccess
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForIndexing
- AWSBackupServiceRolePolicyForItemRestores
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSBackupServiceRolePolicyForScans
- AWSBatchFullAccess
- AWSBatchServiceEventTargetRole
- AWSBatchServiceRole
- AWSBatchServiceRolePolicyForSageMaker
- AWSBCMDataExportsServiceRolePolicy
- AWSBillingConductorFullAccess
- AWSBillingConductorReadOnlyAccess
- AWSBillingReadOnlyAccess
- AWSBillingServiceRolePolicy
- AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM
- AWSBudgetsActionsWithAWSResourceControlAccess
- AWSBudgetsReadOnlyAccess
- AWSBugBustFullAccess
- AWSBugBustPlayerAccess

- AWSBugBustServiceRolePolicy
- AWSCertificateManagerFullAccess
- AWSCertificateManagerPrivateCAAuditor
- AWSCertificateManagerPrivateCAFullAccess
- AWSCertificateManagerPrivateCAPrivilegedUser
- AWSCertificateManagerPrivateCAReadOnly
- AWSCertificateManagerPrivateCAUser
- AWSCertificateManagerReadOnly
- AWSChatbotServiceLinkedRolePolicy
- AWSCleanRoomsFullAccess
- AWSCleanRoomsFullAccessNoQuerying
- AWSCleanRoomsMLFullAccess
- AWSCleanRoomsMLReadOnlyAccess
- AWSCleanRoomsReadOnlyAccess
- AWSCleanRoomsServiceRolePolicy
- AWSCloud9Administrator
- AWSCloud9EnvironmentMember
- AWSCloud9ServiceRolePolicy
- AWSCloud9SSMInstanceProfile
- AWSCloud9User
- AWSCloudFormationFullAccess
- AWSCloudFormationReadOnlyAccess
- AWSCloudFrontLogger
- AWSCloudFrontVPCOriginServiceRolePolicy
- AWSCloudHSMFullAccess
- AWSCloudHSMReadOnlyAccess
- AWSCloudHSMRole
- AWSCloudMapDiscoverInstanceAccess
- AWSCloudMapFullAccess
- AWSCloudMapReadOnlyAccess

- AWSCloudMapRegisterInstanceAccess
- AWSCloudShellFullAccess
- AWSCloudTrail_FullAccess
- AWSCloudTrail_ReadOnlyAccess
- AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy
- AWSCodeArtifactAdminAccess
- AWSCodeArtifactReadOnlyAccess
- AWSCodeBuildAdminAccess
- AWSCodeBuildDeveloperAccess
- AWSCodeBuildReadOnlyAccess
- AWSCodeCommitFullAccess
- AWSCodeCommitPowerUser
- AWSCodeCommitReadOnly
- AWSCodeDeployDeployerAccess
- AWSCodeDeployFullAccess
- AWSCodeDeployReadOnlyAccess
- AWSCodeDeployRole
- AWSCodeDeployRoleForCloudFormation
- AWSCodeDeployRoleForECS
- AWSCodeDeployRoleForECSLimited
- AWSCodeDeployRoleForLambda
- AWSCodeDeployRoleForLambdaLimited
- AWSCodePipeline_FullAccess
- AWSCodePipeline_ReadOnlyAccess
- AWSCodePipelineApproverAccess
- AWSCodePipelineCustomActionAccess
- AWSCodeStarFullAccess
- AWSCodeStarNotificationsServiceRolePolicy
- AWSCodeStarServiceRole
- AWSCompromisedKeyQuarantine

- AWSCompromisedKeyQuarantineV2
- AWSCompromisedKeyQuarantineV3
- AWSConfigMultiAccountSetupPolicy
- AWSConfigRemediationServiceRolePolicy
- AWSConfigRoleForOrganizations
- AWSConfigRulesExecutionRole
- AWSConfigServiceRolePolicy
- AWSConfigUserAccess
- AWSConnector
- AWSControlTowerAccountServiceRolePolicy
- AWSControlTowerCloudTrailRolePolicy
- AWSControlTowerIdentityCenterManagementPolicy
- AWSControlTowerServiceRolePolicy
- AWSCostAndUsageReportAutomationPolicy
- AWSDataExchangeDataGrantOwnerFullAccess
- AWSDataExchangeDataGrantReceiverFullAccess
- AWSDataExchangeFullAccess
- AWSDataExchangeProviderFullAccess
- AWSDataExchangeReadOnly
- AWSDataExchangeServiceRolePolicyForLicenseManagement
- AWSDataExchangeServiceRolePolicyForOrganizationDiscovery
- AWSDataExchangeSubscriberFullAccess
- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccess
- AWSDataPipeline_FullAccess
- AWSDataPipeline_PowerUser
- AWSDataSyncDiscoveryServiceRolePolicy
- AWSDataSyncFullAccess
- AWSDataSyncReadOnlyAccess

- AWSDataSyncServiceRolePolicy
- AWSDeadlineCloud-FleetWorker
- AWSDeadlineCloud-UserAccessFarms
- AWSDeadlineCloud-UserAccessFleets
- AWSDeadlineCloud-UserAccessJobs
- AWSDeadlineCloud-UserAccessQueues
- AWSDeadlineCloud-WorkerHost
- AWSDeepLensLambdaFunctionAccessPolicy
- AWSDeepLensServiceRolePolicy
- AWSDeepRacerAccountAdminAccess
- AWSDeepRacerCloudFormationAccessPolicy
- AWSDeepRacerDefaultMultiUserAccess
- AWSDeepRacerFullAccess
- AWSDeepRacerRoboMakerAccessPolicy
- AWSDeepRacerServiceRolePolicy
- AWSDenyAll
- AWSDeviceFarmFullAccess
- AWSDeviceFarmServiceRolePolicy
- AWSDeviceFarmTestGridServiceRolePolicy
- AWSDirectConnectFullAccess
- AWSDirectConnectReadOnlyAccess
- AWSDirectConnectServiceRolePolicy
- AWSDirectoryServiceDataFullAccess
- AWSDirectoryServiceDataReadOnlyAccess
- AWSDirectoryServiceFullAccess
- AWSDirectoryServiceReadOnlyAccess
- AWSDirectoryServiceServiceRolePolicy
- AWSDiscoveryContinuousExportFirehosePolicy
- AWSDMSFleetAdvisorServiceRolePolicy
- AWSDMSServerlessServiceRolePolicy

- AWSEC2CapacityManagerServiceRolePolicy
- AWSEC2CapacityReservationFleetRolePolicy
- AWSEC2FleetServiceRolePolicy
- AWSEC2SpotFleetServiceRolePolicy
- AWSEC2SpotServiceRolePolicy
- AWSEC2SqlHaInstancePolicy
- AWSEC2SqlHaServiceRolePolicy
- AWSEC2VssSnapshotPolicy
- AWSECRPullThroughCache_ServiceRolePolicy
- AWSElasticBeanstalkCustomPlatformforEC2Role
- AWSElasticBeanstalkEnhancedHealth
- AWSElasticBeanstalkMaintenance
- AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy
- AWSElasticBeanstalkManagedUpdatesServiceRolePolicy
- AWSElasticBeanstalkMulticontainerDocker
- AWSElasticBeanstalkReadOnly
- AWSElasticBeanstalkRoleCore
- AWSElasticBeanstalkRoleCWL
- AWSElasticBeanstalkRoleECS
- AWSElasticBeanstalkRoleRDS
- AWSElasticBeanstalkRoleSNS
- AWSElasticBeanstalkRoleWorkerTier
- AWSElasticBeanstalkService
- AWSElasticBeanstalkServiceRolePolicy
- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticDisasterRecoveryAgentInstallationPolicy
- AWSElasticDisasterRecoveryAgentPolicy
- AWSElasticDisasterRecoveryConsoleFullAccess
- AWSElasticDisasterRecoveryConsoleFullAccess_v2

- AWSElasticDisasterRecoveryConversionServerPolicy
- AWSElasticDisasterRecoveryCrossAccountReplicationPolicy
- AWSElasticDisasterRecoveryEc2InstancePolicy
- AWSElasticDisasterRecoveryFailbackInstallationPolicy
- AWSElasticDisasterRecoveryFailbackPolicy
- AWSElasticDisasterRecoveryLaunchActionsPolicy
- AWSElasticDisasterRecoveryNetworkReplicationPolicy
- AWSElasticDisasterRecoveryReadOnlyAccess
- AWSElasticDisasterRecoveryRecoveryInstancePolicy
- AWSElasticDisasterRecoveryReplicationServerPolicy
- AWSElasticDisasterRecoveryServiceRolePolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy
- AWSElasticDisasterRecoveryStagingAccountPolicy_v2
- AWSElasticLoadBalancingClassicServiceRolePolicy
- AWSElasticLoadBalancingServiceRolePolicy
- AWSElementalMediaConnectFullAccess
- AWSElementalMediaConnectReadOnlyAccess
- AWSElementalMediaConvertFullAccess
- AWSElementalMediaConvertReadOnly
- AWSElementalMediaLiveFullAccess
- AWSElementalMediaLiveReadOnly
- AWSElementalMediaPackageFullAccess
- AWSElementalMediaPackageReadOnly
- AWSElementalMediaPackageV2FullAccess
- AWSElementalMediaPackageV2ReadOnly
- AWSElementalMediaStoreFullAccess
- AWSElementalMediaStoreReadOnly
- AWSElementalMediaTailorFullAccess
- AWSElementalMediaTailorReadOnly
- AWSEnhancedClassicNetworkingMangementPolicy

- AWSEntityResolutionConsoleFullAccess
- AWSEntityResolutionConsoleReadOnlyAccess
- AWSFaultInjectionSimulatorEC2Access
- AWSFaultInjectionSimulatorECSAccess
- AWSFaultInjectionSimulatorEKSAccess
- AWSFaultInjectionSimulatorNetworkAccess
- AWSFaultInjectionSimulatorRDSAccess
- AWSFaultInjectionSimulatorSSMAccess
- AWSFinSpaceServiceRolePolicy
- AWSFMAdminFullAccess
- AWSFMAdminReadOnlyAccess
- AWSFMMemberReadOnlyAccess
- AWSForWordPressPluginPolicy
- AWSGitSyncServiceRolePolicy
- AWSGlobalAcceleratorSLRPolicy
- AWSGlueConsoleFullAccess
- AWSGlueConsoleSageMakerNotebookFullAccess
- AwsGlueDataBrewFullAccessPolicy
- AWSGlueDataBrewServiceRole
- AWSGlueSchemaRegistryFullAccess
- AWSGlueSchemaRegistryReadonlyAccess
- AWSGlueServiceNotebookRole
- AWSGlueServiceRole
- AwsGlueSessionUserRestrictedNotebookPolicy
- AwsGlueSessionUserRestrictedNotebookServiceRole
- AwsGlueSessionUserRestrictedPolicy
- AwsGlueSessionUserRestrictedServiceRole
- AWSGrafanaAccountAdministrator
- AWSGrafanaConsoleReadOnlyAccess
- AWSGrafanaWorkspacePermissionManagement

- AWSGrafanaWorkspacePermissionManagementV2
- AWSGreengrassFullAccess
- AWSGreengrassReadOnlyAccess
- AWSGreengrassResourceAccessRolePolicy
- AWSGroundStationAgentInstancePolicy
- AWSHealth_EventProcessorServiceRolePolicy
- AWSHealthFullAccess
- AWSHealthImagingFullAccess
- AWSHealthImagingReadOnlyAccess
- AWSIAMIdentityCenterAllowListForIdentityContext
- AWSIdentityCenterExternalManagementPolicy
- AWSIdentitySyncFullAccess
- AWSIdentitySyncReadOnlyAccess
- AWSImageBuilderFullAccess
- AWSImageBuilderReadOnlyAccess
- AWSImportExportFullAccess
- AWSImportExportReadOnlyAccess
- AWSIncidentManagerIncidentAccessServiceRolePolicy
- AWSIncidentManagerResolverAccess
- AWSIncidentManagerServiceRolePolicy
- AWSIoT1ClickFullAccess
- AWSIoT1ClickReadOnlyAccess
- AWSIoTAnalyticsFullAccess
- AWSIoTAnalyticsReadOnlyAccess
- AWSIoTConfigAccess
- AWSIoTConfigReadOnlyAccess
- AWSIoTDataAccess
- AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction
- AWSIoTDeviceDefenderAudit
- AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

- AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction
- AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction
- AWSIoTDeviceDefenderUpdateCACertMitigationAction
- AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction
- AWSIoTDeviceTesterForFreeRTOSFullAccess
- AWSIoTDeviceTesterForGreengrassFullAccess
- AWSIoTEventsFullAccess
- AWSIoTEventsReadOnlyAccess
- AWSIoTFleetHubFederationAccess
- AWSIoTFleetwiseServiceRolePolicy
- AWSIoTFullAccess
- AWSIoTLogging
- AWSIoTManagedIntegrationsFullAccess
- AWSIoTManagedIntegrationsRolePolicy
- AWSIoTOTAUpdate
- AWSIotRoboRunnerFullAccess
- AWSIotRoboRunnerReadOnly
- AWSIotRoboRunnerServiceRolePolicy
- AWSIoTRuleActions
- AWSIoTSiteWiseConsoleFullAccess
- AWSIoTSiteWiseFullAccess
- AWSIoTSiteWiseMonitorPortalAccess
- AWSIoTSiteWiseMonitorServiceRolePolicy
- AWSIoTSiteWiseReadOnlyAccess
- AWSIoTThingsRegistration
- AWSIoTTwinMakerServiceRolePolicy
- AWSIoTWirelessDataAccess
- AWSIoTWirelessFullAccess
- AWSIoTWirelessFullPublishAccess
- AWSIoTWirelessGatewayCertManager

- AWSIoTWirelessLogging
- AWSIoTWirelessReadOnlyAccess
- AWSIPAMServiceRolePolicy
- AWSIQContractServiceRolePolicy
- AWSIQFullAccess
- AWSIQPermissionServiceRolePolicy
- AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy
- AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy
- AWSKeyManagementServicePowerUser
- AWSLakeFormationCrossAccountManager
- AWSLakeFormationDataAdmin
- AWSLambda_FullAccess
- AWSLambda_ReadOnlyAccess
- AWSLambdaBasicDurableExecutionRolePolicy
- AWSLambdaBasicExecutionRole
- AWSLambdaDynamoDBExecutionRole
- AWSLambdaENIManagementAccess
- AWSLambdaExecute
- AWSLambdaFullAccess
- AWSLambdaInvocation-DynamoDB
- AWSLambdaKinesisExecutionRole
- AWSLambdaManagedEC2ResourceOperator
- AWSLambdaMSKExecutionRole
- AWSLambdaReplicator
- AWSLambdaRole
- AWSLambdaServiceRolePolicy
- AWSLambdaSQSQueueExecutionRole
- AWSLambdaVPCAccessExecutionRole
- AWSLicenseManagerConsumptionPolicy
- AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

- AWSLicenseManagerMasterAccountRolePolicy
- AWSLicenseManagerMemberAccountRolePolicy
- AWSLicenseManagerServiceRolePolicy
- AWSLicenseManagerUserSubscriptionsServiceRolePolicy
- AWSM2ServicePolicy
- AWSManagedServices_ContactsServiceRolePolicy
- AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy
- AWSManagedServices_EventsServiceRolePolicy
- AWSManagedServices_SelfServiceReporting_ServiceRolePolicy
- AWSManagedServicesDeploymentToolkitPolicy
- AWSManagementConsoleAdministratorAccess
- AWSManagementConsoleBasicUserAccess
- AWSMarketplaceAmiIngestion
- AWSMarketplaceDeploymentServiceRolePolicy
- AWSMarketplaceFullAccess
- AWSMarketplaceGetEntitlements
- AWSMarketplaceImageBuildFullAccess
- AWSMarketplaceLicenseManagementServiceRolePolicy
- AWSMarketplaceManageSubscriptions
- AWSMarketplaceMeteringFullAccess
- AWSMarketplaceMeteringRegisterUsage
- AWSMarketplaceProcurementSystemAdminFullAccess
- AWSMarketplacePurchaseOrdersServiceRolePolicy
- AWSMarketplaceRead-only
- AWSMarketplaceResaleAuthorizationServiceRolePolicy
- AWSMarketplaceSellerFullAccess
- AWSMarketplaceSellerOfferManagement
- AWSMarketplaceSellerProductsFullAccess
- AWSMarketplaceSellerProductsReadOnly
- AWSMcpServiceActionsFullAccess

- AWSMediaConnectServicePolicy
- AWSMediaLiveAnywhereServiceRolePolicy
- AWSMediaTailorServiceRolePolicy
- AWSMigrationHubDiscoveryAccess
- AWSMigrationHubDMSAccess
- AWSMigrationHubFullAccess
- AWSMigrationHubOrchestratorConsoleFullAccess
- AWSMigrationHubOrchestratorInstanceRolePolicy
- AWSMigrationHubOrchestratorPlugin
- AWSMigrationHubOrchestratorServiceRolePolicy
- AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess
- AWSMigrationHubRefactorSpaces-SSMAutomationPolicy
- AWSMigrationHubRefactorSpacesFullAccess
- AWSMigrationHubRefactorSpacesServiceRolePolicy
- AWSMigrationHubSMSAccess
- AWSMigrationHubStrategyCollector
- AWSMigrationHubStrategyConsoleFullAccess
- AWSMigrationHubStrategyServiceRolePolicy
- AWSMobileHub_FullAccess
- AWSMobileHub_ReadOnly
- AWSMSKReplicatorExecutionRole
- AWSNATGatewayServiceRolePolicy
- AWSNetworkFirewallFullAccess
- AWSNetworkFirewallReadOnlyAccess
- AWSNetworkFirewallServiceRolePolicy
- AWSNetworkManagerCloudWANServiceRolePolicy
- AWSNetworkManagerFullAccess
- AWSNetworkManagerReadOnlyAccess
- AWSNetworkManagerServiceRolePolicy
- AWSObservabilityAdminLogsCentralizationServiceRolePolicy

- AWSObservabilityAdminServiceRolePolicy
- AWSObservabilityAdminTelemetryEnablementServiceRolePolicy
- AWSOrganizationsFullAccess
- AWSOrganizationsReadOnlyAccess
- AWSOrganizationsServiceTrustPolicy
- AWSOutpostsAuthorizeServerPolicy
- AWSOutpostsServiceRolePolicy
- AWSPanoramaApplianceRolePolicy
- AWSPanoramaApplianceServiceRolePolicy
- AWSPanoramaFullAccess
- AWSPanoramaGreengrassGroupRolePolicy
- AWSPanoramaSageMakerRolePolicy
- AWSPanoramaServiceLinkedRolePolicy
- AWSPanoramaServiceRolePolicy
- AWSPartnerCentralChannelHandshakeApprovalManagement
- AWSPartnerCentralChannelManagement
- AWSPartnerCentralFullAccess
- AWSPartnerCentralMarketingManagement
- AWSPartnerCentralOpportunityManagement
- AWSPartnerCentralSandboxFullAccess
- AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy
- AWSPartnerLedSupportReadOnlyAccess
- AWSPCSComputeNodePolicy
- AWSPCSServiceRolePolicy
- AWSPriceListServiceFullAccess
- AWSPrivateCAAuditor
- AWSPrivateCAConnectorForKubernetesPolicy
- AWSPrivateCAFullAccess
- AWSPrivateCAPrivilegedUser
- AWSPrivateCAReadOnly

- AWSPrivateCAUser
- AWSPrivateMarketplaceAdminFullAccess
- AWSPrivateMarketplaceRequests
- AWSPrivateNetworksServiceRolePolicy
- AWSProtonCodeBuildProvisioningBasicAccess
- AWSProtonCodeBuildProvisioningServiceRolePolicy
- AWSProtonDeveloperAccess
- AWSProtonFullAccess
- AWSProtonReadOnlyAccess
- AWSProtonServiceGitSyncServiceRolePolicy
- AWSProtonSyncServiceRolePolicy
- AWSPurchaseOrdersServiceRolePolicy
- AWSQuickSetupCFGCPacksPermissionsBoundary
- AWSQuickSetupDeploymentRolePolicy
- AWSQuickSetupDevOpsGuruPermissionsBoundary
- AWSQuickSetupDistributorPermissionsBoundary
- AWSQuickSetupEnableAREXExecutionPolicy
- AWSQuickSetupEnableDHMCExecutionPolicy
- AWSQuickSetupJITNADeploymentRolePolicy
- AWSQuickSetupManagedInstanceProfileExecutionPolicy
- AWSQuickSetupManageJITNAResourcesExecutionPolicy
- AWSQuickSetupPatchPolicyBaselineAccess
- AWSQuickSetupPatchPolicyDeploymentRolePolicy
- AWSQuickSetupPatchPolicyPermissionsBoundary
- AWSQuickSetupSchedulerPermissionsBoundary
- AWSQuickSetupSSMDeploymentRolePolicy
- AWSQuickSetupSSMDeploymentS3BucketRolePolicy
- AWSQuickSetupSSMHostMgmtPermissionsBoundary
- AWSQuickSetupSSMLifecycleManagementExecutionPolicy
- AWSQuickSetupSSMManageResourcesExecutionPolicy

- AWSQuickSetupStartSSMAssociationsExecutionPolicy
- AWSQuickSetupStartStopInstancesExecutionPolicy
- AWSQuickSightAssetBundleExportPolicy
- AWSQuickSightAssetBundleImportPolicy
- AWSQuicksightAthenaAccess
- AWSQuickSightDescribeRDS
- AWSQuickSightDescribeRedshift
- AWSQuickSightElasticsearchPolicy
- AWSQuickSightIoTAnalyticsAccess
- AWSQuickSightListIAM
- AWSQuicksightOpenSearchPolicy
- AWSQuickSightSageMakerPolicy
- AWSQuickSightSecretsManagerWriteAccess
- AWSQuickSightSecretsManagerWritePolicy
- AWSQuickSightTimestreamPolicy
- AWSReachabilityAnalyzerServiceRolePolicy
- AWSRefactoringToolkitFullAccess
- AWSRefactoringToolkitSidecarPolicy
- AWSrePostPrivateCloudWatchAccess
- AWSRepostSpaceSupportOperationsPolicy
- AWSResilienceHubAsssessmentExecutionPolicy
- AWSResourceAccessManagerFullAccess
- AWSResourceAccessManagerReadOnlyAccess
- AWSResourceAccessManagerResourceShareParticipantAccess
- AWSResourceAccessManagerServiceRolePolicy
- AWSResourceExplorerFullAccess
- AWSResourceExplorerOrganizationsAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy
- AWSResourceGroupsReadOnlyAccess

- AWSRoboMaker_FullAccess
- AWSRoboMakerReadOnlyAccess
- AWSRoboMakerServicePolicy
- AWSRoboMakerServiceRolePolicy
- AWSRolesAnywhereFullAccess
- AWSRolesAnywhereReadOnly
- AWSRolesAnywhereServicePolicy
- AWSS3OnOutpostsServiceRolePolicy
- AWSSavingsPlansFullAccess
- AWSSavingsPlansReadOnlyAccess
- AWSSecretsManagerClientReadOnlyAccess
- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess
- AWSSecurityHubReadOnlyAccess
- AWSSecurityHubServiceRolePolicy
- AWSSecurityHubV2ServiceRolePolicy
- AWSSecurityIncidentResponseCaseFullAccess
- AWSSecurityIncidentResponseFullAccess
- AWSSecurityIncidentResponseReadOnlyAccess
- AWSSecurityIncidentResponseServiceRolePolicy
- AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWSServiceCatalogAdminFullAccess
- AWSServiceCatalogAdminReadOnlyAccess
- AWSServiceCatalogAppRegistryFullAccess
- AWSServiceCatalogAppRegistryReadOnlyAccess
- AWSServiceCatalogAppRegistryServiceRolePolicy
- AWSServiceCatalogEndUserFullAccess
- AWSServiceCatalogEndUserReadOnlyAccess
- AWSServiceCatalogOrgsDataSyncServiceRolePolicy
- AWSServiceCatalogSyncServiceRolePolicy

- AWSServiceRoleForAmazonEKSNodegroup
- AWSServiceRoleForAmazonQDeveloper
- AWSServiceRoleForAWSTransform
- AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy
- AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy
- AWSServiceRoleForCodeGuru-Profiler
- AWSServiceRoleForCodeWhispererPolicy
- AWSServiceRoleForEC2ScheduledInstances
- AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy
- AWSServiceRoleForImageBuilder
- AWSServiceRoleForIoTSiteWise
- AWSServiceRoleForLogDeliveryPolicy
- AWSServiceRoleForMonitronPolicy
- AWSServiceRoleForNeptuneGraphPolicy
- AWSServiceRoleForPrivateMarketplaceAdminPolicy
- AWSServiceRoleForProcurementInsightsPolicy
- AWSServiceRoleForSMS
- AWSServiceRoleForUserSubscriptions
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting
- AWSServiceRolePolicyForWorkspacesInstances
- AWSShieldDRTAccessPolicy
- AWSShieldServiceRolePolicy
- AWSSocialMessagingServiceRolePolicy
- AWSSSMForSAPServiceLinkedRolePolicy
- AWSSSMOpsInsightsServiceRolePolicy
- AWSSSODirectoryAdministrator
- AWSSSODirectoryReadOnly
- AWSSSOMasterAccountAdministrator
- AWSSSOMemberAccountAdministrator

- AWSSSOReadOnly
- AWSSSOServiceRolePolicy
- AWSStepFunctionsConsoleFullAccess
- AWSStepFunctionsFullAccess
- AWSStepFunctionsReadOnlyAccess
- AWSStorageGatewayFullAccess
- AWSStorageGatewayReadOnlyAccess
- AWSStorageGatewayServiceRolePolicy
- AWSSupplyChainFederationAdminAccess
- AWSSupportAccess
- AWSSupportAppFullAccess
- AWSSupportAppReadOnlyAccess
- AWSSupportPlansFullAccess
- AWSSupportPlansReadOnlyAccess
- AWSSupportServiceRolePolicy
- AWSSystemsManagerAccountDiscoveryServicePolicy
- AWSSystemsManagerChangeManagementServicePolicy
- AWSSystemsManagerEnableConfigRecordingExecutionPolicy
- AWSSystemsManagerEnableExplorerExecutionPolicy
- AWSSystemsManagerForSAPFullAccess
- AWSSystemsManagerForSAPReadOnlyAccess
- AWSSystemsManagerJustInTimeAccessServicePolicy
- AWSSystemsManagerJustInTimeAccessTokenPolicy
- AWSSystemsManagerJustInTimeAccessTokenSessionPolicy
- AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy
- AWSSystemsManagerNotificationsServicePolicy
- AWSSystemsManagerOpsDataSyncServiceRolePolicy
- AWSThinkboxAssetServerPolicy
- AWSThinkboxAWSPortalAdminPolicy
- AWSThinkboxAWSPortalGatewayPolicy

- AWSThinkboxAWSPortalWorkerPolicy
- AWSThinkboxDeadlineResourceTrackerAccessPolicy
- AWSThinkboxDeadlineResourceTrackerAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginAdminPolicy
- AWSThinkboxDeadlineSpotEventPluginWorkerPolicy
- AWSTransferConsoleFullAccess
- AWSTransferFullAccess
- AWSTransferLoggingAccess
- AWSTransferReadOnlyAccess
- AWSTransformApplicationDeploymentPolicy
- AWSTransformApplicationECSDeploymentPolicy
- AWSTransformCustomExecuteTransformations
- AWSTransformCustomFullAccess
- AWSTransformCustomManageTransformations
- AWSTrustedAdvisorPriorityFullAccess
- AWSTrustedAdvisorPriorityReadOnlyAccess
- AWSTrustedAdvisorReportingServiceRolePolicy
- AWSTrustedAdvisorServiceRolePolicy
- AWSUserAttributeCostAllocationPolicy
- AWSUserNotificationsServiceLinkedRolePolicy
- AWSVendorInsightsAssessorFullAccess
- AWSVendorInsightsAssessorReadOnly
- AWSVendorInsightsVendorFullAccess
- AWSVendorInsightsVendorReadOnly
- AWSVpcLatticeServiceRolePolicy
- AWSVPCS2SVpnServiceRolePolicy
- AWSVPCTransitGatewayServiceRolePolicy
- AWSVPCVerifiedAccessServiceRolePolicy
- AWSWAFConsoleFullAccess
- AWSWAFConsoleReadOnlyAccess

- AWSWAFFullAccess
- AWSWAFReadOnlyAccess
- AWSWellArchitectedDiscoveryServiceRolePolicy
- AWSWellArchitectedOrganizationsServiceRolePolicy
- AWSWickrFullAccess
- AWSXrayCrossAccountSharingConfiguration
- AWSXRayDaemonWriteAccess
- AWSXrayFullAccess
- AWSXrayReadOnlyAccess
- AWSXrayWriteOnlyAccess
- AWSZonalAutoshiftPracticeRunSLRPolicy
- AWSZoneGroupAccessManagementServiceRolePolicy
- BatchServiceRolePolicy
- BedrockAgentCoreFullAccess
- BedrockAgentCoreNetworkServiceRolePolicy
- BedrockAgentCoreRuntimeIdentityServiceRolePolicy
- Billing
- BudgetsServiceRolePolicy
- CertificateManagerServiceRolePolicy
- ClientVPNServiceConnectionsRolePolicy
- ClientVPNServiceRolePolicy
- CloudFormationStackSetsOrgAdminServiceRolePolicy
- CloudFormationStackSetsOrgMemberServiceRolePolicy
- CloudFrontFullAccess
- CloudFrontReadOnlyAccess
- CloudHSMServiceRolePolicy
- CloudSearchFullAccess
- CloudSearchReadOnlyAccess
- CloudTrailEventContext
- CloudTrailServiceRolePolicy

- CloudWatch-CrossAccountAccess
- CloudWatchActionsEC2Access
- CloudWatchAgentAdminPolicy
- CloudWatchAgentServerPolicy
- CloudWatchApplicationInsightsFullAccess
- CloudWatchApplicationInsightsReadOnlyAccess
- CloudwatchApplicationInsightsServiceLinkedRolePolicy
- CloudWatchApplicationSignalsFullAccess
- CloudWatchApplicationSignalsReadOnlyAccess
- CloudWatchApplicationSignalsServiceRolePolicy
- CloudWatchAutomaticDashboardsAccess
- CloudWatchCrossAccountSharingConfiguration
- CloudWatchEventsBuiltInTargetExecutionAccess
- CloudWatchEventsFullAccess
- CloudWatchEventsInvocationAccess
- CloudWatchEventsReadOnlyAccess
- CloudWatchEventsServiceRolePolicy
- CloudWatchFullAccess
- CloudWatchFullAccessV2
- CloudWatchInternetMonitorFullAccess
- CloudWatchInternetMonitorReadOnlyAccess
- CloudWatchInternetMonitorServiceRolePolicy
- CloudWatchLambdaApplicationSignalsExecutionRolePolicy
- CloudWatchLambdaInsightsExecutionRolePolicy
- CloudWatchLogsCrossAccountSharingConfiguration
- CloudWatchLogsFullAccess
- CloudWatchLogsReadOnlyAccess
- CloudWatchNetworkFlowMonitorAgentPublishPolicy
- CloudWatchNetworkFlowMonitorServiceRolePolicy
- CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

- CloudWatchNetworkMonitorServiceRolePolicy
- CloudWatchOpenSearchDashboardAccess
- CloudWatchOpenSearchDashboardsFullAccess
- CloudWatchReadOnlyAccess
- CloudWatchSyntheticsFullAccess
- CloudWatchSyntheticsReadOnlyAccess
- ComprehendDataAccessRolePolicy
- ComprehendFullAccess
- ComprehendMedicalFullAccess
- ComprehendReadOnly
- ComputeOptimizerAutomationServiceRolePolicy
- ComputeOptimizerReadOnlyAccess
- ComputeOptimizerServiceRolePolicy
- ConfigConformsServiceRolePolicy
- ConsoleFullAccessFromVercel
- ConsoleViewOnlyAccessFromVercel
- CostOptimizationHubAdminAccess
- CostOptimizationHubReadOnlyAccess
- CostOptimizationHubServiceRolePolicy
- CustomerProfilesServiceLinkedRolePolicy
- DatabaseAdministrator
- DataScientist
- DAXServiceRolePolicy
- DeclarativePoliciesEC2Report
- DynamoDBCloudWatchContributorInsightsServiceRolePolicy
- DynamoDBGlobalTableSettingsManagementServiceRolePolicy
- DynamoDBKinesisReplicationServiceRolePolicy
- DynamoDBReplicationServiceRolePolicy
- EC2FastLaunchFullAccess
- EC2FastLaunchServiceRolePolicy

- EC2FleetTimeShiftableServiceRolePolicy
- Ec2ImageBuilderCrossAccountDistributionAccess
- EC2ImageBuilderLifecycleExecutionPolicy
- EC2InstanceConnect
- Ec2InstanceConnectEndpoint
- EC2InstanceProfileForImageBuilder
- EC2InstanceProfileForImageBuilderECRContainerBuilds
- ECRReplicationServiceRolePolicy
- ECRTemplateServiceRolePolicy
- ElastiCacheServiceRolePolicy
- ElasticLoadBalancingFullAccess
- ElasticLoadBalancingReadOnly
- ElementalActivationsDownloadSoftwareAccess
- ElementalActivationsFullAccess
- ElementalActivationsGenerateLicenses
- ElementalActivationsReadOnlyAccess
- ElementalAppliancesSoftwareFullAccess
- ElementalAppliancesSoftwareReadOnlyAccess
- ElementalSupportCenterFullAccess
- EMRDescribeClusterPolicyForEMRWAL
- FMSServiceRolePolicy
- FSxDeleteServiceLinkedRoleAccess
- GameLiftContainerFleetPolicy
- GameLiftGameServerGroupPolicy
- GitLabDuoWithAmazonQPermissionsPolicy
- GlobalAcceleratorFullAccess
- GlobalAcceleratorReadOnlyAccess
- GreengrassOTAUpdateArtifactAccess
- GroundTruthSyntheticConsoleFullAccess
- GroundTruthSyntheticConsoleReadOnlyAccess

- Health_OrganizationsServiceRolePolicy
- IAMAccessAdvisorReadOnly
- IAMAccessAnalyzerFullAccess
- IAMAccessAnalyzerReadOnlyAccess
- IAMFullAccess
- IAMReadOnlyAccess
- IAMSelfManageServiceSpecificCredentials
- IAMUserChangePassword
- IAMUserSSHKeys
- IVSFullAccess
- IVSReadOnlyAccess
- IVSRecordToS3
- KafkaConnectServiceRolePolicy
- KafkaServiceRolePolicy
- KeyspacesCDCServiceRolePolicy
- KeyspacesReplicationServiceRolePolicy
- LakeFormationDataAccessServiceRolePolicy
- LexBotPolicy
- LexChannelPolicy
- LightsailExportAccess
- MediaConnectGatewayInstanceRolePolicy
- MediaPackageServiceRolePolicy
- MemoryDBServiceRolePolicy
- MigrationHubDMSAccessServiceRolePolicy
- MigrationHubServiceRolePolicy
- MigrationHubSMSAccessServiceRolePolicy
- MonitronServiceRolePolicy
- MultiPartyApprovalFullAccess
- MultiPartyApprovalReadOnlyAccess
- NeptuneConsoleFullAccess

- NeptuneFullAccess
- NeptuneGraphReadOnlyAccess
- NeptuneReadOnlyAccess
- NetworkAdministrator
- NetworkSecurityDirectorServiceLinkedRolePolicy
- NovaActServiceRolePolicy
- OAMFullAccess
- OAMReadOnlyAccess
- OpensearchIngestionSelfManagedVpcePolicy
- PartnerCentralAccountManagementUserRoleAssociation
- PowerUserAccess
- QAppsServiceRolePolicy
- QBusinessQuicksightPluginPolicy
- QBusinessServiceRolePolicy
- QuickSightAccessForS3StorageManagementAnalyticsReadOnly
- RDSCloudHsmAuthorizationRole
- ReadOnlyAccess
- ResourceGroupsandTagEditorFullAccess
- ResourceGroupsandTagEditorReadOnlyAccess
- ResourceGroupsServiceRolePolicy
- ResourceGroupsTaggingAPITagUntagSupportedResources
- ROSAAmazonEBSCSIDriverOperatorPolicy
- ROSACloudNetworkConfigOperatorPolicy
- ROSAControlPlaneOperatorPolicy
- ROSAImageRegistryOperatorPolicy
- ROSAIngressOperatorPolicy
- ROSAInstallerPolicy
- ROSAKMSProviderPolicy
- ROSAKubeControllerPolicy
- ROSAManageSubscription

- ROSANodePoolManagementPolicy
- ROSASharedVPCEndpointPolicy
- ROSASharedVPCRoute53Policy
- ROSASRESupportPolicy
- ROSAWorkerInstancePolicy
- Route53RecoveryReadinessServiceRolePolicy
- Route53ResolverServiceRolePolicy
- RTBFabricServiceRolePolicy
- S3StorageLensServiceRolePolicy
- SageMakerStudioAdminIAMConsolePolicy
- SageMakerStudioAdminIAMDefaultExecutionPolicy
- SageMakerStudioAdminIAMPermissiveExecutionPolicy
- SageMakerStudioAdminProjectUserRolePolicy
- SageMakerStudioBedrockAgentServiceRolePolicy
- SageMakerStudioBedrockChatAgentUserRolePolicy
- SageMakerStudioBedrockEvaluationJobServiceRolePolicy
- SageMakerStudioBedrockFlowServiceRolePolicy
- SageMakerStudioBedrockFunctionExecutionRolePolicy
- SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy
- SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy
- SageMakerStudioBedrockPromptUserRolePolicy
- SageMakerStudioDomainExecutionRolePolicy
- SageMakerStudioDomainServiceRolePolicy
- SageMakerStudioEMRContainersSystemNamespaceRolePolicy
- SageMakerStudioEMRInstanceRolePolicy
- SageMakerStudioEMRServiceRolePolicy
- SageMakerStudioFullAccess
- SageMakerStudioProjectProvisioningRolePolicy
- SageMakerStudioProjectRoleMachineLearningPolicy
- SageMakerStudioProjectUserRolePermissionsBoundary

- SageMakerStudioProjectUserRolePolicy
- SageMakerStudioQueryExecutionRolePolicy
- SageMakerStudioUserIAMConsolePolicy
- SageMakerStudioUserIAMDefaultExecutionPolicy
- SageMakerStudioUserIAMPermissiveExecutionPolicy
- SecretsManagerReadWrite
- SecurityAgentWebAppAPIPolicy
- SecurityAudit
- SecurityLakeResourceManagementServiceRolePolicy
- SecurityLakeServiceLinkedRole
- ServerMigration_ServiceRole
- ServerMigrationConnector
- ServerMigrationServiceConsoleFullAccess
- ServerMigrationServiceLaunchRole
- ServerMigrationServiceRoleForInstanceValidation
- ServiceQuotasFullAccess
- ServiceQuotasReadOnlyAccess
- ServiceQuotasServiceRolePolicy
- SignInLocalDevelopmentAccess
- SimpleWorkflowFullAccess
- SMSVoiceServiceRolePolicy
- SplitCostAllocationDataServiceRolePolicy
- SSMQuickSetupRolePolicy
- SupportUser
- SystemAdministrator
- TranslateFullAccess
- TranslateReadOnly
- ViewOnlyAccess
- VMImportExportRoleForAWSConnector
- VPCLatticeFullAccess

- VPCLatticeReadOnlyAccess
- VPCLatticeServicesInvokeAccess
- WAFLoggingServiceRolePolicy
- WAFRegionalLoggingServiceRolePolicy
- WAFV2LoggingServiceRolePolicy
- WellArchitectedConsoleFullAccess
- WellArchitectedConsoleReadOnlyAccess
- WorkLinkServiceRolePolicy

AccessAnalyzerServiceRolePolicy

Beschreibung: Erlauben Sie Access Analyzer, Ressourcenmetadaten zu analysieren

`AccessAnalyzerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Dezember 2019, 17:13 Uhr UTC
- Bearbeitete Zeit: 12. Mai 2025, 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AccessAnalyzerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessAnalyzerServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ecr:DescribeRepositories",
        "ecr:GetAccountSetting",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListEntitiesForPolicy",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetUser",
        "iam:GetGroup",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails",
        "iam:ListAccessKeys",
        "iam:GetLoginProfile",
        "iam:GetAccessKeyLastUsed",
        "iam:ListRolePolicies",
```

```
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListUserPolicies",
        "iam:GetUserPolicy",
        "iam:ListAttachedUserPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListGroupsForUser",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListVersionsByFunction",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
```

```
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3express:GetAccessPoint",
        "s3express:GetAccessPointPolicy",
        "s3express:GetBucketPolicy",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:ListAccessPointsForDirectoryBuckets",
        "sns:GetTopicAttributes",
        "sns:ListTopics",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AccountManagementFromVercel

Beschreibung: Zur Verwendung mit Konten, die über die Vercel Marketplace-Integration mit AWS erstellt wurden. Bietet Zugriff auf Kontoverwaltung, Benachrichtigung, Kosten- und Nutzungsanalyse sowie Identitätsanbieterverwaltung.

`AccountManagementFromVercel`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AccountManagementFromVercel` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2025, 16:34 UTC
- Bearbeitete Zeit: 11. Dezember 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AccountManagementFromVercel`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:CloseAccount",
        "bcm-recommended-actions:ListRecommendedActions",
        "ce:GetCostAndUsage",
        "cur:GetUsageReport",
        "iam:ListSAMLProviders",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSamlProvider",
        "iam:GetSamlProvider"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VercelInstallId" : "${aws:PrincipalTag/VercelInstallId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess

Beschreibung: Bietet vollen Zugriff auf AWS Dienste und Ressourcen.

`AdministratorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC

- ARN: `arn:aws:iam::aws:policy/AdministratorAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess-Amplify

Beschreibung: Gewährt dem Konto Administratorrechte und ermöglicht gleichzeitig ausdrücklich den direkten Zugriff auf Ressourcen, die von Amplify-Anwendungen benötigt werden.

`AdministratorAccess-Amplify`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AdministratorAccess-Amplify` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 19:03 UTC
- Bearbeitete Zeit: 4. April 2024, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-Amplify`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CLICloudformationPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackSet",
        "cloudformation:UpdateStackSet",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*"
      ]
    },
    {
      "Sid" : "CLIManageviaCFNPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:UpdateRole",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "iam:ListPolicyVersions",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:CreateRole",
        "iam:ListRolePolicies",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary",
        "appsync:CreateApiKey",
        "appsync:CreateDataSource",
        "appsync:CreateFunction",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteApiKey",
```

```
        "appsync:DeleteDataSource",
        "appsync:DeleteFunction",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetDataSource",
        "appsync:GetFunction",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetType",
        "appsync:GraphQL",
        "appsync:ListApiKeys",
        "appsync:ListDataSources",
        "appsync:ListFunctions",
        "appsync:ListGraphqlApis",
        "appsync:ListResolvers",
        "appsync:ListResolversByFunction",
        "appsync:ListTypes",
        "appsync:StartSchemaCreation",
        "appsync:UntagResource",
        "appsync:UpdateApiKey",
        "appsync:UpdateDataSource",
        "appsync:UpdateFunction",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:CreateGraphqlApi",
        "appsync:DeleteGraphqlApi",
        "appsync:GetGraphqlApi",
        "appsync:ListTagsForResource",
        "appsync:UpdateGraphqlApi",
        "apigateway:DELETE",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "cognito-idp:CreateUserPool",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:DescribeIdentity",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:UpdateIdentityPool",
```

```
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-identity:TagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:SetUserPoolMfaConfig",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeAsync",
        "lambda:InvokeFunction",
        "lambda:RemovePermission",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:AddLayerVersionPermission",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteLayerVersion",
        "lambda:GetEventSourceMapping",
        "lambda:GetLayerVersion",
        "lambda:ListEventSourceMappings",
        "lambda:ListLayerVersions",
        "lambda:PublishLayerVersion",
        "lambda:RemoveLayerVersionPermission",
        "lambda:UpdateEventSourceMapping",
        "dynamodb:CreateTable",
        "dynamodb:DeleteItem",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
```

```
        "dynamodb:ListStreams",
        "dynamodb:PutItem",
        "dynamodb:TagResource",
        "dynamodb:ListTagsOfResource",
        "dynamodb:UntagResource",
        "dynamodb:UpdateContinuousBackups",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable",
        "dynamodb:UpdateTimeToLive",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketWebsite",
        "s3:PutObjectAcl",
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:DeleteCloudFrontOriginAccessIdentity",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:UpdateCloudFrontOriginAccessIdentity",
        "cloudfront:UpdateDistribution",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "mobiletargeting:GetApp",
        "kinesis:AddTagsToStream",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListTagsForStream",
        "kinesis:PutRecords",
        "es:AddTags",
```

```
        "es:CreateElasticsearchDomain",
        "es:DeleteElasticsearchDomain",
        "es:DescribeElasticsearchDomain",
        "es:UpdateElasticsearchDomainConfig",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CLISDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetIntrospectionSchema",
        "appsync:GraphQL",
        "appsync:UpdateApiKey",
        "appsync:ListApiKeys",
        "amplify:*",
        "amplifybackend:*",
        "amplifyuibuilder:*",
        "sts:AssumeRole",
        "mobiletargeting:*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:CreateGroup",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUser",
        "cognito-idp:ListUsers",
        "cognito-idp:AdminGetUser",
        "cognito-idp:ListUsersInGroup",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:AdminResetUserPassword",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:ListGroups",
        "cognito-idp:AdminListUserAuthEvents",
        "cognito-idp:AdminDeleteUser",
```

```
        "cognito-idp:AdminConfirmSignUp",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminUpdateUserAttributes",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:AdminSetUserPassword",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:DeleteIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:DeleteLayerVersion",
        "lambda:InvokeFunction",
        "lambda:ListLayerVersions",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListAttachedRolePolicies",
        "iam:CreateRole",
        "iam:PassRole",
        "iam:ListRolePolicies",
        "iam:DeleteRolePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "cloudformation:ListStacks",
```

```
        "cloudformation:DescribeStacks",
        "sns:CreateSMSSandboxPhoneNumber",
        "sns:GetSMSSandboxAccountStatus",
        "sns:VerifySMSSandboxPhoneNumber",
        "sns:DeleteSMSSandboxPhoneNumber",
        "sns:ListSMSSandboxPhoneNumbers",
        "sns:ListOriginationNumbers",
        "rekognition:DescribeCollection",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "lex:GetBot",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "cloudformation:GetTemplateSummary",
        "codecommit:GitPull",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetCloudFrontOriginAccessIdentityConfig",
        "polly:DescribeVoices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSMCalls",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*"
    },
    {
      "Sid" : "GeoPowerUser",
      "Effect" : "Allow",
      "Action" : [
        "geo:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AmplifyEcrSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifyStorageSDKCalls",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteBucketWebsite",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRCalls",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:CreateCloudFrontOriginAccessIdentity",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
```

```
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByLambdaFunction",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListInvalidations",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListStreamingDistributions",
        "cloudfront:UpdateDistribution",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudfront:ListTagsForResource",
        "cloudfront:DeleteDistribution",
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:PutRolePolicy",
        "iam:PassRole",
        "lambda:CreateFunction",
        "lambda:EnableReplication",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "s3:CreateBucket",
        "s3:GetAccelerateConfiguration",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutObject",
        "s3:PutBucketTagging",
        "s3:GetBucketTagging",
        "lambda:ListEventSourceMappings",
```

```
        "lambda:CreateEventSourceMapping",
        "iam:UpdateAssumeRolePolicy",
        "iam:DeleteRolePolicy",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:UpdateApp",
        "amplify:UpdateBranch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmplifySSRViewLogGroups",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "arn:aws:logs:*:*:log-group:*"
    },
    {
      "Sid" : "AmplifySSRCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*"
    },
    {
      "Sid" : "AmplifySSRPushLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/amplify/*:log-stream:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AdministratorAccess-AWSElasticBeanstalk

Beschreibung: Gewährt dem Konto Administratorrechte. Ermöglicht Entwicklern und Administratoren ausdrücklich den direkten Zugriff auf Ressourcen, die sie für die Verwaltung von AWS Elastic Beanstalk Beanstalk-Anwendungen benötigen

`AdministratorAccess-AWSElasticBeanstalk`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AdministratorAccess-AWSElasticBeanstalk` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Januar 2021, 19:36 UTC
- Bearbeitete Zeit: 12. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AdministratorAccess-AWSElasticBeanstalk`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:Describe*",
        "acm:List*",
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:Validate*",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "codecommit:Get*",
        "codecommit:UploadArchive",
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate*",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroup*",
        "ecs:CreateCluster",
        "ecs:DeRegisterTaskDefinition",
        "ecs:Describe*",
        "ecs:List*",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:Describe*",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "logs:Describe*",
```

```
        "rds:Describe*",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:*"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:SignalResource",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/Elastic-Beanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:TagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/awseb-e-*",
        "arn:aws:dynamodb:*:*:table/eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*Rule",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetSecurityGroups"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:*"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
```

```
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/eb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/awseb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/*/eb-*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/eb-*/*/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-elasticbeanstalk*",
        "arn:aws:iam::*:instance-profile/aws-elasticbeanstalk*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk*",
      "Condition" : {
        "ArnLike" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::aws:policy/AWSElasticBeanstalk*",
            "arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalk*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
```

```
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/autoscaling.amazonaws.com/
AWSServiceRoleForAutoScaling*",
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*",
        "arn:aws:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing*",
        "arn:aws:iam::*:role/aws-service-role/
managedupdates.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*",
        "arn:aws:iam::*:role/aws-service-role/
maintenance.elasticbeanstalk.amazonaws.com/AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "elasticbeanstalk.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "managedupdates.elasticbeanstalk.amazonaws.com",
            "maintenance.elasticbeanstalk.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
```

```
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*DBSubnetGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBInstance",
        "rds:DeleteDBSecurityGroup",
        "rds:ModifyDBInstance",
        "rds:RestoreDBInstanceFromDBSnapshot"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:secgrp:eb-*",
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:subgrp:awseb-e-*",
        "arn:aws:rds:*:*:subgrp:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketOwnershipControls"
      ],
```

```
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:*QueueAttributes",
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:SendMessage",
        "sqs:TagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AIOpsAssistantIncidentReportPolicy

Beschreibung: Stellt die Berechtigungen bereit, die der Amazon AI Operations Assistant benötigt, um einen Vorfallbericht über die Untersuchung zu erstellen.

`AIOpsAssistantIncidentReportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AIOpsAssistantIncidentReportPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Oktober 2025, 22:04 UTC
- Bearbeitete Zeit: 10. Oktober 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantIncidentReportPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GetReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "aiops:GetFact",
        "aiops:ListFacts",
        "aiops:GetFactVersions",
        "aiops:GetInvestigation",
        "aiops:ListInvestigationEvents",
        "aiops:GetInvestigationEvent"
      ],
      "Resource" : [
        "arn:aws:aiops:*:*:investigation-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AIOpsAssistantPolicy

Beschreibung: Stellt die ReadOnly Berechtigungen bereit, die der Amazon AI Operations Assistant benötigt, um bei Untersuchungen Analysen der AWS Kundenressourcen durchzuführen.

`AIOpsAssistantPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AIOpsAssistantPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Dezember 2024, 16:21 UTC
- Bearbeitete Zeit: 17. Dezember 2025, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsAssistantPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOPSServiceAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:List*",
        "acm-pca:Describe*",
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:List*",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "airflow:List*",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:List*",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:List*",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetEnvironment",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:List*",
        "appflow:Describe*",
        "appflow:List*",
        "application-autoscaling:Describe*",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:List*",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "apprunner:Describe*",
        "apprunner:List*",
        "appstream:Describe*",
        "appstream:List*",
        "appsync:GetApiAssociation",
        "appsync:GetDataSource",
        "appsync:GetDomainName",
```

```
        "appsync:GetFunction",
        "appsync:GetGraphqlApi",
        "appsync:GetIntrospectionSchema",
        "appsync:GetResolver",
        "appsync:GetSourceApiAssociation",
        "appsync:List*",
        "aps:Describe*",
        "aps:List*",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:List*",
        "athena:GetCapacityAssignmentConfiguration",
        "athena:GetCapacityReservation",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAssessment",
        "auditmanager:List*",
        "autoscaling:Describe*",
        "backup-gateway:GetHypervisor",
        "backup-gateway:List*",
        "backup:Describe*",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:List*",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:List*",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataSource",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:List*",
        "budgets:Describe*",
        "budgets:List*",
```

```
        "ce:Describe*",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:List*",
        "chatbot:Describe*",
        "chatbot:GetMicrosoftTeamsChannelConfiguration",
        "chatbot:List*",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:List*",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:List*",
        "cloudformation:Describe*",
        "cloudformation:GetResource",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:List*",
        "cloudfront:Describe*",
        "cloudfront:GetCachePolicy",
        "cloudfront:GetCloudFrontOriginAccessIdentity",
        "cloudfront:GetContinuousDeploymentPolicy",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetFunction",
        "cloudfront:GetKeyGroup",
        "cloudfront:GetMonitoringSubscription",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetOriginRequestPolicy",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:List*",
        "cloudtrail:Describe*",
        "cloudtrail:GetChannel",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetQueryResults",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrail",
```

```
        "cloudtrail:GetTrailStatus",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartQuery",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetInsightRuleReport",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricStream",
        "cloudwatch:GetService",
        "cloudwatch:GetServiceLevelObjective",
        "cloudwatch:List*",
        "codeartifact:Describe*",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:List*",
        "codebuild:BatchGetFleets",
        "codebuild:List*",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:GetApplication",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:List*",
        "codeguru-profiler:Describe*",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:List*",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:List*",
        "codestar-notifications:Describe*",
        "codestar-notifications:List*",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
```

```
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:AdminListGroupsForUser",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetLogDeliveryConfiguration",
        "cognito-idp:GetUICustomization",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:GetWebACLForResource",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListTagsForResource",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:GetStoredQuery",
        "config:List*",
        "connect:Describe*",
        "connect:GetTaskTemplate",
        "connect:List*",
        "databrew:Describe*",
        "databrew:List*",
        "datapipeline:Describe*",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:List*",
        "datasync:Describe*",
        "datasync:List*",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetStorageProfile",
```

```
        "deadline:List*",
        "detective:GetMembers",
        "detective:List*",
        "devicefarm:GetDevicePool",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:GetVPCEConfiguration",
        "devicefarm:List*",
        "devops-guru:Describe*",
        "devops-guru:GetResourceCollection",
        "devops-guru:List*",
        "dms:Describe*",
        "dms:List*",
        "ds:Describe*",
        "dynamodb:Describe*",
        "dynamodb:GetResourcePolicy",
        "dynamodb:List*",
        "ec2:Describe*",
        "ec2:GetAssociatedEnclaveCertificateIamRoles",
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessEndpointPolicy",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr:Describe*",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
```

```
        "elasticache:List*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:GetResourcePolicy",
        "elasticloadbalancing:GetTrustStoreCaCertificatesBundle",
        "elasticloadbalancing:GetTrustStoreRevocationContent",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "emr-containers:Describe*",
        "emr-containers:List*",
        "emr-serverless:GetApplication",
        "emr-serverless:List*",
        "es:Describe*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:List*",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:List*",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:List*",
        "forecast:Describe*",
        "forecast:List*",
        "frauddetector:BatchGetVariable",
        "frauddetector:Describe*",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
```

```
        "frauddetector:GetModelVersion",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:List*",
        "fsx:Describe*",
        "gamelift:Describe*",
        "gamelift:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetJob",
        "glue:GetRegistry",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:List*",
        "glue:querySchemaVersionMetadata",
        "grafana:Describe*",
        "grafana:List*",
        "greengrass:Describe*",
        "greengrass:GetDeployment",
        "greengrass:List*",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:List*",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:List*",
        "health:DescribeEvents",
        "health:DescribeEventDetails",
        "healthlake:Describe*",
        "healthlake:List*",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
```

```
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListOpenIDConnectProviders",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:GetWorkflow",
        "imagebuilder:List*",
        "inspector2:List*",
        "inspector:Describe*",
        "inspector:List*",
        "internetmonitor:GetMonitor",
        "internetmonitor:List*",
        "iot:Describe*",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetThingShadow",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
```

```
        "iot:GetV2LoggingOptions",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotevents:Describe*",
        "iotevents:List*",
        "iotfleethub:Describe*",
        "iotfleethub:List*",
        "iotsitewise:Describe*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:List*",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:List*",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:List*",
        "kafka:Describe*",
        "kafka:GetClusterPolicy",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:Describe*",
        "kendra:List*",
        "kinesis:Describe*",
        "kinesis:GetResourcePolicy",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kms:DescribeKey",
        "kms:ListResourceTags",
```

```
        "kms:ListKeys",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeyRotations",
        "lakeformation:Describe*",
        "lakeformation:GetLFTag",
        "lakeformation:GetResourceLFTags",
        "lakeformation:List*",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetFunctionRecursionConfig",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:List*",
        "launchwizard:GetDeployment",
        "launchwizard:List*",
        "lex:Describe*",
        "lex:List*",
        "license-manager:GetLicense",
        "license-manager:List*",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetInstance",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:Describe*",
        "logs:FilterLogEvents",
```

```
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:List*",
        "lookoutvision:Describe*",
        "lookoutvision:List*",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:List*",
        "macie2:GetAllowList",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsFilter",
        "macie2:GetMacieSession",
        "macie2:List*",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:Describe*",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:List*",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
```

```
        "mediapackagev2:List*",
        "memorydb:Describe*",
        "memorydb:List*",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:List*",
        "mq:Describe*",
        "mq:List*",
        "network-firewall:Describe*",
        "network-firewall:List*",
        "networkmanager:Describe*",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
        "networkmanager:GetVpcAttachment",
        "networkmanager:List*",
        "nimble:GetLaunchProfile",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:List*",
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:List*",
        "omics:GetAnnotationStore",
        "omics:GetReferenceStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:List*",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "organizations:Describe*",
```

```
        "organizations:List*",
        "osis:GetPipeline",
        "osis:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:List*",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:List*",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:List*",
        "personalize:Describe*",
        "personalize:List*",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pipes:Describe*",
        "pipes:List*",
        "proton:GetEnvironmentTemplate",
        "proton:GetServiceTemplate",
        "proton:List*",
        "qbusiness:GetApplication",
        "qbusiness:GetDataSource",
        "qbusiness:GetIndex",
        "qbusiness:GetPlugin",
        "qbusiness:GetRetriever",
        "qbusiness:GetWebExperience",
        "qbusiness:List*",
        "qldb:Describe*",
        "qldb:List*",
        "ram:GetPermission",
        "ram:List*",
        "rds:Describe*",
        "rds:List*",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "refactor-spaces:GetApplication",
```

```
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetRoute",
        "refactor-spaces:List*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetView",
        "resource-explorer-2:List*",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:List*",
        "robomaker:Describe*",
        "robomaker:List*",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:List*",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:List*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:List*",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetOutpostResolver",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:List*",
        "rum:GetAppMonitor",
```

```
        "rum:List*",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:List*",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketMetadataTableConfiguration",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "S3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
```

```
            "s3:List*",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:List*",
            "schemas:Describe*",
            "schemas:GetResourcePolicy",
            "schemas:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "securityhub:BatchGetAutomationRules",
            "securityhub:BatchGetSecurityControls",
            "securityhub:Describe*",
            "securityhub:GetConfigurationPolicy",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:GetEnabledStandards",
            "securityhub:GetFindingAggregator",
            "securityhub:GetInsights",
            "securityhub:List*",
            "securitylake:GetSubscriber",
            "securitylake:List*",
            "servicecatalog:Describe*",
            "servicecatalog:GetApplication",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:List*",
            "servicequotas:GetServiceQuota",
            "ses:Describe*",
            "ses:GetAccount",
            "ses:GetAddonInstance",
            "ses:GetAddonSubscription",
            "ses:GetArchive",
            "ses:GetConfigurationSet",
            "ses:GetConfigurationSetEventDestinations",
            "ses:GetContactList",
            "ses:GetDedicatedIpPool",
            "ses:GetDedicatedIps",
            "ses:GetEmailIdentity",
            "ses:GetEmailTemplate",
            "ses:GetIngressPoint",
            "ses:GetRelay",
            "ses:GetRuleSet",
            "ses:GetTemplate",
```

```
        "ses:GetTrafficPolicy",
        "ses:List*",
        "shield:Describe*",
        "shield:List*",
        "signer:GetSigningProfile",
        "signer:List*",
        "sns:GetDataProtectionPolicy",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:List*",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:List*",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:List*",
        "ssm-sap:GetApplication",
        "ssm-sap:List*",
        "ssm:Describe*",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetParameters",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:List*",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:GetSharedSsoConfiguration",
        "sso:ListAccountAssignments",
        "sso:ListApplicationAssignments",
        "sso:ListApplications",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListTagsForResource",
        "states:GetExecutionHistory",
        "states:Describe*",
        "states:List*",
```

```
        "synthetics:Describe*",
        "synthetics:GetCanary",
        "synthetics:GetGroup",
        "synthetics:List*",
        "tag:GetResources",
        "timestream:Describe*",
        "timestream:List*",
        "transfer:Describe*",
        "transfer:List*",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:List*",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:List*",
        "wafv2:GetIPSet",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRegexPatternSet",
        "wafv2:GetRuleGroup",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:List*",
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:List*",
        "workspaces:Describe*",
        "xray:BatchGetTraces",
```

```
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AIOPSS3AccessForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amplify",
        "arn:aws:s3:::cdk--assets--*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ViaAWSService" : [
            "amplify.amazonaws.com"
          ],
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "AIOPSAPIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integrations/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/domainnames/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AIOpsConsoleAdminPolicy

Beschreibung: Gewährt über die AWS Konsole vollen Zugriff auf den Amazon AI Operations Service und die erforderlichen Berechtigungen. Es beinhaltet auch Berechtigungen zur Verwendung identitätsbewusster Konsolensitzungen.

`AIOpsConsoleAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AIOpsConsoleAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 02. Dezember 2024, 23:51 UTC
- Bearbeitete Zeit: 17. November 2025, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsConsoleAdminPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "aiops:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:PutApplicationAccessScope",
        "sso:PutApplicationAssignmentConfiguration",
```

```
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        }
      }
    },
    {
      "Sid" : "SSOApplicationTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:TagResource"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/aiops"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:RequestTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:TagResource"
      ],
      "Resource" : "arn:aws:sso::*:application/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "aiops.amazonaws.com",
          "aws:ResourceTag/ManagedByAmazonAIOperations" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ManagedByAmazonAIOperations"
          ]
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:ListApplications",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:DescribeInstance",
        "sso:GetSSOStatus",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "IdentityPropagationAccess",
      "Effect" : "Allow",
      "Action" : [
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudtrailAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListEventDataStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMIntegrationSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:aws/ssm/3p/*"
    },
    {
      "Sid" : "SSMIntegrationAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationCreatePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/service-role/
AWSServiceRoleSSMIntegrationsPolicy*"
    },
```

```
    {
      "Sid" : "ChatbotConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackWorkspaces",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:ListMicrosoftTeamsConfiguredTeams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToAIOps",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "aiops.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagBoundaryPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleToSSMIntegration",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.integrations.amazonaws.com"
        },
        "ArnEquals" : {
          "iam:AssociatedResourceArn" : "arn:aws:aiops:*:*:investigation-group/*"
        }
      }
    },
    {
      "Sid" : "SSMOpsItemAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:*:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : "CloudWatch",
          "aws:ResourceTag/Integration" : "CloudWatch"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Integration"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAIOpsCrossAccountAssistantPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreatePolicy"
      ],
      "Resource" : "arn:aws:iam::*:policy/AIOpsCrossAccountAssistantPolicy*"
    },
    {
      "Sid" : "AmazonQAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AIOpsOperatorAccess

Beschreibung: Gewährt Zugriff auf Amazon AI Operations APIs zum Erstellen, Aktualisieren und Löschen von Untersuchungen, Ermittlungsereignissen und Ermittlungsressourcen. Es beinhaltet auch ReadOnly den Zugriff auf alle KI-Operationen APIs und die Nutzung identitätsbewusster Sitzungen.

`AIOpsOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AIOpsOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Dezember 2024, 23:51 UTC
- Bearbeitete Zeit: 7. November 2025, 22:49 UTC

- ARN: `arn:aws:iam::aws:policy/AIOpsOperatorAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsOperatorAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:CreateInvestigation",
        "aiops:CreateInvestigationEvent",
        "aiops:CreateInvestigationResource",
        "aiops:DeleteInvestigation",
        "aiops:Get*",
        "aiops:List*",
        "aiops:UpdateInvestigation",
        "aiops:UpdateInvestigationEvent",
        "aiops:ValidateInvestigationGroup",
        "aiops:PutFact",
        "aiops:UpdateReport",
        "aiops:GenerateReport",
        "aiops:CreateReport",
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSTSContextSetting",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMSettingServiceIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/integrations/*"
    },
    {
      "Sid" : "SSMIntegrationTagAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
```

```
      }
    },
    {
      "Sid" : "SSMOpsItemIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        }
      }
    },
    {
      "Sid" : "SSMTagOperation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Integration" : [
            "CloudWatch"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Integration"
        }
      }
    },
    {
      "Sid" : "SSMOpsSummaryIntegration",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AIOpsReadOnlyAccess

Beschreibung: Erteilt dem Amazon AI Operations-Service und den erforderlichen Ressourcen ReadOnly Berechtigungen.

`AIOpsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AIOpsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Dezember 2024, 23:51 UTC
- Bearbeitete Zeit: 24. Juni 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/AIOpsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AIOpsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aiops:Get*",
        "aiops:List*",
        "aiops:ValidateInvestigationGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "sso:DescribeInstance",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessDeviceSetup

Beschreibung: Bieten Sie beim Geräte-Setup Zugriff auf AlexaForBusiness Dienste

`AlexaForBusinessDeviceSetup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessDeviceSetup` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 20. Mai 2019, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessDeviceSetup`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterDevice",
        "a4b:CompleteRegistration",
        "a4b:SearchDevices",
        "a4b:SearchNetworkProfiles",
        "a4b:GetNetworkProfile",
        "a4b:PutDeviceSetupEvents"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "A4bDeviceSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessFullAccess

Beschreibung: Gewährt vollen Zugriff auf AlexaForBusiness Ressourcen und Zugriff auf verwandte AWS-Services

`AlexaForBusinessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Bearbeitete Zeit: 1. Juli 2020, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:*",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "*a4b.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*a4b.amazonaws.com/
AWSServiceRoleForAlexaForBusiness*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4B*"
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "A4B*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessGatewayExecution

Beschreibung: Stellen Sie Gateway-Ausführungszugriff auf AlexaForBusiness Dienste bereit

`AlexaForBusinessGatewayExecution`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessGatewayExecution` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Zeit bearbeitet: 30. November 2017, 16:47 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessGatewayExecution`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Send*",
        "a4b:Get*"
      ],
      "Resource" : "arn:aws:a4b:*:*:gateway/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
```

```
        "sqs:DeleteMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:dd-*",
        "arn:aws:sqs:*:*:sd-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:List*",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessLifesizeDelegatedAccessPolicy

Beschreibung: Ermöglichen Sie den Zugriff auf Lifesize AVS-Geräte

`AlexaForBusinessLifesizeDelegatedAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessLifesizeDelegatedAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2020, 19:46 UTC
- Bearbeitete Zeit: 12. Juni 2020, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessLifesizeDelegatedAccessPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A2IWO7UEGWV4TL"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "a4b:filters_deviceType" : [
            "*A2IWO7UEGWV4TL"
          ]
        },
        "Null" : {
          "a4b:filters_deviceType" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A2IWO7UEGWV4TL",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:GetRoom",
        "a4b:GetAddressBook",
```

```
        "a4b:SearchRooms",
        "a4b:CreateContact",
        "a4b:CreateRoom",
        "a4b:UpdateContact",
        "a4b:ListConferenceProviders",
        "a4b:DeleteRoom",
        "a4b:CreateAddressBook",
        "a4b:DisassociateContactFromAddressBook",
        "a4b:CreateConferenceProvider",
        "a4b:PutConferencePreference",
        "a4b:DeleteAddressBook",
        "a4b:AssociateContactWithAddressBook",
        "a4b:DeleteContact",
        "a4b:SearchProfiles",
        "a4b:UpdateProfile",
        "a4b:GetContact"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessNetworkProfileServicePolicy

Beschreibung: Diese Richtlinie ermöglicht es Alexa for Business, automatisierte Aufgaben auszuführen, die von Ihren Netzwerkprofilen geplant sind.

`AlexaForBusinessNetworkProfileServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. März 2019, 00:53 UTC
- Bearbeitete Zeit: 5. April 2019, 21:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AlexaForBusinessNetworkProfileServicePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "A4bPcaTagAccess",
```

```
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate",
        "acm-pca:RevokeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/a4b" : "enabled"
        }
      }
    },
    {
      "Sid" : "A4bNetworkProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:A4BNetworkProfile*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessPolyDelegatedAccessPolicy

Beschreibung: Ermöglichen Sie den Zugriff auf Poly AVS-Geräte

`AlexaForBusinessPolyDelegatedAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessPolyDelegatedAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Oktober 2019, 19:48 UTC
- Bearbeitete Zeit: 16. Oktober 2019, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessPolyDelegatedAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "a4b:DisassociateDeviceFromRoom",
        "a4b:DeleteDevice",
        "a4b:UpdateDevice",
        "a4b:GetDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD"
      ]
    },
    {
      "Action" : [
        "a4b:RegisterAVSDevice"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "a4b:amazonId" : [
            "A238TWV36W3S92",
            "A1FUZ1SC53VJXD"
          ]
        }
      }
    },
    {
      "Action" : [
        "a4b:SearchDevices"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "a4b:AssociateDeviceWithRoom"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:a4b:us-east-1:*:device/*/*:A238TWV36W3S92",
        "arn:aws:a4b:us-east-1:*:device/*/*:A1FUZ1SC53VJXD",
        "arn:aws:a4b:us-east-1:*:room/*"
      ]
    },
    {
      "Action" : [
        "a4b:GetRoom",
        "a4b:SearchRooms",
        "a4b:CreateRoom",
        "a4b:GetProfile",
        "a4b:SearchSkillGroups",
        "a4b:DisassociateSkillGroupFromRoom",
        "a4b:AssociateSkillGroupWithRoom",
        "a4b:GetSkillGroup",
        "a4b:SearchProfiles",
        "a4b:GetAddressBook",
        "a4b:UpdateRoom"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AlexaForBusinessReadOnlyAccess

Beschreibung: Bieten Sie nur Lesezugriff auf AlexaForBusiness Dienste

`AlexaForBusinessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AlexaForBusinessReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:47 UTC
- Zeit bearbeitet: 20. November 2019, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AlexaForBusinessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayAdministrator

Beschreibung: Bietet vollen Zugriff auf create/edit/delete APIs in Amazon API Gateway über die AWS-Managementkonsole.

`AmazonAPIGatewayAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAPIGatewayAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:34 Uhr UTC
- Zeit bearbeitet: 9. Juli 2015, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayAdministrator`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:*"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayInvokeFullAccess

Beschreibung: Bietet vollen Zugriff zum Aufrufen APIs in Amazon API Gateway.

`AmazonAPIGatewayInvokeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAPIGatewayInvokeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:36 Uhr UTC
- Bearbeitete Zeit: 18. Dezember 2018, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAPIGatewayInvokeFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : "arn:aws:execute-api:*:*:*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAPIGatewayPushToCloudWatchLogs

Beschreibung: Ermöglicht API Gateway, Protokolle an das Benutzerkonto zu senden.

`AmazonAPIGatewayPushToCloudWatchLogs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAPIGatewayPushToCloudWatchLogs` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. November 2015, 23:41 Uhr UTC
- Zeit bearbeitet: 11. November 2015, 23:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppFlowFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon AppFlow und Zugriff auf AWS Dienste, die als Flow-Quelle oder -Ziel (S3 und Redshift) unterstützt werden. Bietet auch Zugriff auf KMS zur Verschlüsselung

`AmazonAppFlowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppFlowFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juni 2020, 23:30 Uhr UTC
- Bearbeitete Zeit: 28. Februar 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appflow:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesForRedshift",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "KMSListGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "S3PutBucketPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::appflow-*"
    },
    {
      "Sid" : "SecretsManagerCreateSecretAccess",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
```

```
    {
      "Sid" : "LambdaListFunctions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppFlowReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Appflow Flows

`AmazonAppFlowReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppFlowReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juni 2020, 23:26 UTC
- Bearbeitete Zeit: 28. Februar 2022, 20:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppFlowReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnector",
        "appflow:DescribeConnectors",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlows",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListConnectorFields",
        "appflow:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

Beschreibung: Erteilt dem ARC-Regional-Switch Berechtigungen zur Planausführung und Planauswertung.

`AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. November 2025, 19:34 UTC
- Zeit bearbeitet: 03. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource" : "*",
      "Sid" : "GetPlanAndExecutions"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:SimulatePrincipalPolicy",
      "Resource" : "arn:aws:iam::*:role/*",
      "Sid" : "PlanEvaluation"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*",
      "Sid" : "CloudWatch"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon AppStream über die AWS-Managementkonsole.

`AmazonAppStreamFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppStreamFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 28. August 2020, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "appstream:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScheduledActions",
```

```
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:ListRoles",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
ApplicationAutoScalingForAmazonAppStreamAccess",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appstream.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_AppStreamFleet",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "appstream.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamPCAAccess

Beschreibung: Amazon AppStream 2.0-Zugriff auf AWS Certificate Manager Private CA in Kundenkonten für zertifikatsbasierte Authentifizierung

`AmazonAppStreamPCAAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppStreamPCAAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. Oktober 2022, 17:05 UTC
- Bearbeitete Zeit: 24. Oktober 2022, 17:05 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamPCAAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon AppStream über die AWS-Managementkonsole.

`AmazonAppStreamReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppStreamReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 22. Oktober 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAppStreamReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:List*",
        "appstream:Describe*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAppStreamServiceAccess

Beschreibung: Standardrichtlinie für die AppStream Amazon-Servicerolle.

`AmazonAppStreamServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAppStreamServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. November 2016, 04:17 Uhr UTC
- Zeit bearbeitet: 17. November 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonAppStreamServiceAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::appstream2-36fb080bb8-*",
        "arn:aws:s3:::appstream-app-settings-*",
        "arn:aws:s3:::appstream-logs-*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAthenaFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Athena und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für das Abfragen, Schreiben von Ergebnissen und Datenmanagement erforderlich sind.

`AmazonAthenaFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonAthenaFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 16:46 UTC
- Zeit bearbeitet: 03. Januar 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAthenaFullAccess`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
```

```
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:StartColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCatalogImportStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseQueryResultsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Sid" : "BaseAthenaExamplesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::athena-examples*"
      ]
    },
    {
      "Sid" : "BaseS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseSNSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseCloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BaseDataZonePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:ListProjects",
        "datazone:ListAccountEnvironments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BasePricingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAthenaServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon Athena erforderlich sind

`AmazonAthenaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2025, 22:34 UTC
- Bearbeitete Zeit: 14. November 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonAthenaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
```

```
            "AWS/Athena",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIFullAccess

Beschreibung: Bietet Zugriff auf alle Operationen, die Amazon Augmented AI-Ressourcen ausführen können, einschließlich FlowDefinitions, HumanTaskUis und HumanLoops. Erlaubt keinen Zugriff zum Erstellen von FlowDefinitions Inhalten gegen das öffentliche Team.

`AmazonAugmentedAIFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonAugmentedAIFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:21 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIHumanLoopFullAccess

Beschreibung: Ermöglicht den Zugriff zur Ausführung aller Operationen an HumanLoops.

`AmazonAugmentedAIHumanLoopFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAugmentedAIHumanLoopFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:20 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIHumanLoopFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAugmentedAIIntegratedAPIAccess

Beschreibung: Bietet Zugriff auf alle Operationen, die Amazon Augmented AI-Ressourcen ausführen können, einschließlich FlowDefinitions, HumanTaskUis und HumanLoops. Bietet auch Zugriff auf die Operationen von Diensten, die in Amazon Augmented AI integriert sind.

`AmazonAugmentedAIIntegratedAPIAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAugmentedAIIntegratedAPIAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. April 2020, 20:47 UTC
- Bearbeitete Zeit: 22. April 2020, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAugmentedAIIntegratedAPIAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*HumanLoop",
        "sagemaker:*HumanLoops",
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions",
        "sagemaker:*HumanTaskUi",
        "sagemaker:*HumanTaskUis"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectModerationLabels"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAuroraDSQLConsoleFullAccess

Beschreibung: Bietet vollen Administratorzugriff auf Aurora DSQL über die Konsole

`AmazonAuroraDSQLConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAuroraDSQLConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:36 UTC
- Bearbeitete Zeit: 23. Oktober 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
```

```
        "dsql:GetCluster",
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DsqlConsolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ValidatePolicy",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
```

```
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAuroraDSQLFullAccess

Beschreibung: Bietet vollen Administratorzugriff auf Aurora DSQL

`AmazonAuroraDSQLFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAuroraDSQLFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:36 UTC
- Bearbeitete Zeit: 23. Oktober 2025, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DsqlAllPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:PutClusterPolicy",
        "dsql:GetClusterPolicy",
        "dsql:DeleteClusterPolicy",
        "dsql:CreateCluster",
        "dsql:GetCluster",
```

```
        "dsql:UpdateCluster",
        "dsql:DeleteCluster",
        "dsql:ListClusters",
        "dsql:TagResource",
        "dsql:UntagResource",
        "dsql:ListTagsForResource",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:InjectError"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDsqlServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "dsql.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSDescribePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCryptographicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonAuroraDSQLReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Aurora DSQL

`AmazonAuroraDSQLReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonAuroraDSQLReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:21 UTC
- Bearbeitete Zeit: 23. Oktober 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonAuroraDSQLReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DsqlReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetClusterPolicy",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedServicesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRo

Beschreibung: Erteilt Bedrock Model-Inferenzberechtigungen für den Kernspeicher des Bedrock-Agenten

`AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Juli 2025, 13:37 UTC
- Bearbeitete Zeit: 16. Juli 2025, 13:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockAgentCoreMemoryBedrockModelInferenceExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Bedrock sowie eingeschränkten Zugriff auf verwandte Dienste, die von Amazon Bedrock benötigt werden

`AmazonBedrockFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:47 UTC
- Bearbeitete Zeit: 5. Dezember 2025, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
```

```
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
```

```
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Unsubscribe"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockLimitedAccess

Beschreibung: Bietet eingeschränkten Zugriff auf Amazon Bedrock sowie auf zugehörige Dienste, die dafür erforderlich sind

`AmazonBedrockLimitedAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockLimitedAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Juni 2025, 22:22 UTC
- Bearbeitete Zeit: 5. Dezember 2025, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockLimitedAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*",
        "bedrock:CallWithBearerToken",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreateGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreateInferenceProfile",
        "bedrock:CreateModelCopyJob",
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateModelImportJob",
        "bedrock:CreateModelInvocationJob",
        "bedrock:CreatePromptRouter",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:DeleteCustomModel",
        "bedrock:DeleteGuardrail",
        "bedrock:DeleteImportedModel",
        "bedrock:DeleteInferenceProfile",
        "bedrock:DeletePromptRouter",
        "bedrock:DeleteProvisionedModelThroughput",
        "bedrock:StopEvaluationJob",
        "bedrock:StopModelCustomizationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:TagResource",
        "bedrock:UntagResource",
```

```
        "bedrock:UpdateGuardrail",
        "bedrock:UpdateProvisionedModelThroughput",
        "bedrock:ApplyGuardrail",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:*:kms:*:::*"
    },
    {
      "Sid" : "APIsWithAllResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockMantleAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken",
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceOperationsFromBedrockFor3pModels",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:ViewSubscriptions",
```

```
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockMantleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Bedrock Mantle sowie eingeschränkten Zugriff auf verwandte Dienste, die dafür erforderlich sind

`AmazonBedrockMantleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockMantleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2025, 07:19 UTC
- Geänderte Zeit: 4. Dezember 2025, 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleAll",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockMantleInferenceAccess

Beschreibung: Bietet Lese- und Inferenzerstellungszugriff auf Amazon Bedrock Mantle

`AmazonBedrockMantleInferenceAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockMantleInferenceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2025, 07:19 UTC
- Geänderte Zeit: 4. Dezember 2025, 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleInferenceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleInference",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*",
        "bedrock-mantle:CreateInference"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockMantleReadOnly

Beschreibung: Bietet nur Lesezugriff auf Amazon Bedrock Mantle

`AmazonBedrockMantleReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockMantleReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2025, 07:19 UTC
- Geänderte Zeit: 4. Dezember 2025, 07:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMantleReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMantleReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:Get*",
        "bedrock-mantle:List*"
      ],
      "Resource" : "arn:aws:bedrock-mantle:*:*:project/*"
    },
    {
      "Sid" : "BedrockMantleCallWithBearerToken",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-mantle:CallWithBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockMarketplaceAccess

Beschreibung: Bietet eingeschränkten Zugriff auf Amazon Bedrock Marketplace sowie auf zugehörige Dienste, die dafür erforderlich sind

`AmazonBedrockMarketplaceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockMarketplaceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Juni 2025, 22:22 UTC
- Bearbeitete Zeit: 29. Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockMarketplaceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockMarketplaceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateMarketplaceModelEndpoint",
        "bedrock:DeleteMarketplaceModelEndpoint",
        "bedrock:DeregisterMarketplaceModelEndpoint",
        "bedrock:RegisterMarketplaceModelEndpoint",
```

```
        "bedrock:UpdateMarketplaceModelEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointAddTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
```

```
        },
        "StringLike" : {
          "aws:RequestTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:RequestTag/bedrock:marketplace-registration-status" : "registered",
          "aws:RequestTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointDeleteTagsOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker-sdk:bedrock",
            "bedrock:marketplace-registration-status",
            "sagemaker-studio:hub-content-arn"
          ]
        },
        "StringLike" : {
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible",
          "aws:ResourceTag/bedrock:marketplace-registration-status" : "registered",
          "aws:ResourceTag/sagemaker-studio:hub-content-arn" :
"arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
```

```
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MarketplaceModelEndpointInvokingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com",
          "aws:ResourceTag/sagemaker-sdk:bedrock" : "compatible"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
    {
      "Sid" : "AllowMarketplaceModelsListing",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    },
    {
      "Sid" : "PassRoleToSageMaker",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*ForBedrock*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrock",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonBedrock*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Bedrock

`AmazonBedrockReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2023, 15:48 UTC
- Bearbeitete Zeit: 4. Dezember 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonBedrockReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:Get*",
        "bedrock:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceModelEndpointNonMutatingAPIs",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:ListEndpoints",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DiscoveringMarketplaceModel",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeHubContent"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:aws:hub-content/SageMakerPublicHub/Model/*",
        "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
      ]
    },
```

```
    {
      "Sid" : "AllowMarketplaceModelsListing",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListHubContents"
      ],
      "Resource" : "arn:aws:sagemaker:*:aws:hub/SageMakerPublicHub"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBedrockStudioPermissionsBoundary

Beschreibung: Definiert die maximalen Berechtigungen von IAM-Rollen, die Amazon Bedrock Studio für den Betrieb von Amazon Bedrock Studio-Ressourcen erstellt.

`AmazonBedrockStudioPermissionsBoundary`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonBedrockStudioPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. August 2024, 00:24 UTC
- Bearbeitete Zeit: 1. August 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBedrockStudioPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::br-studio-${aws:PrincipalAccount}-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessOpenSearchCollections",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "InvokeBedrockModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*::foundation-model/*"
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:ListTagsForResource",
        "bedrock:TagResource",
        "bedrock:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RetrieveAndGenerate",
      "Effect" : "Allow",
```

```
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "WriteLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "InvokeLambdaFunctions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:br-studio-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretsManagerSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:br-studio/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "UseKmsKeyWithAwsServices",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/EnableBedrock" : "true"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Braket über das AWS-Managementkonsole und SDK. Bietet auch Zugriff auf verwandte Dienste (z. B. S3, Protokolle).

`AmazonBraketFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonBraketFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. August 2020, 20:12 Uhr UTC
- Bearbeitete Zeit: 11. April 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "servicequotas:GetServiceQuota",
        "cloudwatch:GetMetricData",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListNotebookInstances"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/amazon-
braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "braket:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/braket.amazonaws.com/
AWSServiceRoleForAmazonBraket*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "braket.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonBraketServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
```

```
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketJobsExecutionPolicy

Beschreibung: Gewährt Zugriff auf AWS-Services und Ressourcen, die für die Ausführung eines Amazon Braket-Jobs erforderlich sind, einschließlich S3, Cloudwatch, IAM und Braket

`AmazonBraketJobsExecutionPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonBraketJobsExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 26. November 2021, 19:34 UTC
- Bearbeitete Zeit: 28. November 2021, 05:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonBraketJobsExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/amazon-braket*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "braket:CancelJob",
        "braket:CancelQuantumTask",
        "braket:CreateJob",
        "braket:CreateQuantumTask",
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "braket:ListTagsForResource",
        "braket:TagResource",
        "braket:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonBraketJobsExecutionRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "braket.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/braket"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonBraketServiceRolePolicy

Beschreibung: Ermöglicht Amazon Braket, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten

`AmazonBraketServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. August 2020, 17:12 Uhr UTC
- Bearbeitete Zeit: 11. Juli 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonBraketServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::amazon-braket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/braket:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeFullAccess

Beschreibung: Bietet vollen Zugriff auf die Amazon Chime Admin Console über die AWS-Managementkonsole.

`AmazonChimeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonChimeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:15 Uhr UTC
- Bearbeitete Zeit: 14. Dezember 2020, 21:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
```

```
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
```

```
      ]
    },
    {
      "Action" : [
        "kinesis:ListStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-chat-*",
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::chime-chat-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf die Amazon Chime Admin Console über die AWS-Managementkonsole.

`AmazonChimeReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonChimeReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:04 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeReadOnly`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "chime:List*",
        "chime:Get*",
        "chime:Describe*",
        "chime:SearchAvailablePhoneNumbers"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDK

Beschreibung: Bietet Zugriff auf Amazon Chime SDK-Operationen

`AmazonChimeSDK`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonChimeSDK` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Februar 2020, 21:53 UTC
- Bearbeitete Zeit: 10. Januar 2023, 18:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeSDK`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMeeting",
        "chime:CreateMeetingWithAttendees",
        "chime:DeleteMeeting",
        "chime:GetMeeting",
        "chime:ListMeetings",
        "chime:CreateAttendee",
        "chime:BatchCreateAttendee",
        "chime:DeleteAttendee",
        "chime:GetAttendee",
        "chime:ListAttendees",
        "chime:ListAttendeeTags",
        "chime:ListMeetingTags",
        "chime:ListTagsForResource",
        "chime:TagAttendee",
        "chime:TagMeeting",
        "chime:TagResource",
        "chime:UntagAttendee",
        "chime:UntagMeeting",
        "chime:UntagResource",
        "chime:StartMeetingTranscription",
        "chime:StopMeetingTranscription",
        "chime:CreateMediaCapturePipeline",
        "chime:CreateMediaConcatenationPipeline",
        "chime:CreateMediaLiveConnectorPipeline",
        "chime:DeleteMediaCapturePipeline",
        "chime:DeleteMediaPipeline",
        "chime:GetMediaCapturePipeline",
        "chime:GetMediaPipeline",
        "chime:ListMediaCapturePipelines",
        "chime:ListMediaPipelines"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

Beschreibung: Verwaltete Richtlinie für die verknüpfte Rolle mit dem Amazon Chime SDK MediaPipelines Service

`AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. April 2022, 22:02 UTC
- Bearbeitete Zeit: 8. Dezember 2023, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutMetricsForChimeSDKNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ChimeSDK"
        }
      }
    },
    {
      "Sid" : "AllowKinesisVideoStreamsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeMediaPipelines-*"
      ]
    },
    {
      "Sid" : "AllowKinesisVideoStreamsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowChimeMeetingAccess",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetMeeting",
        "chime:CreateAttendee",
        "chime:DeleteAttendee"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeSDKMessagingServiceRolePolicy

Beschreibung: Ermöglicht Amazon Chime SDK Messaging den Zugriff auf AWS Ressourcen und die Aktivierung der Messaging-Funktionalität

`AmazonChimeSDKMessagingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. März 2023, 01:43 UTC
- Bearbeitete Zeit: 03. März 2023, 01:43 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeSDKMessagingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "kinesis.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/chime-messaging-*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die von Amazon Chime verwendet oder verwaltet werden

`AmazonChimeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2019, 22:25 Uhr UTC
- Bearbeitete Zeit: 30. September 2019, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/
AWSServiceRoleForAmazonChime"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "chime.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeTranscriptionServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Chime, in Ihrem Namen auf Amazon Transcribe und Amazon Transcribe Medical zuzugreifen

`AmazonChimeTranscriptionServiceLinkedRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. August 2021, 21:47 UTC
- Bearbeitete Zeit: 4. August 2021, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeTranscriptionServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:StartStreamTranscription",
        "transcribe:StartMedicalStreamTranscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeUserManagement

Beschreibung: Bietet Benutzerverwaltungszugriff auf die Amazon Chime Admin Console über die AWS-Managementkonsole.

`AmazonChimeUserManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonChimeUserManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2017, 22:17 UTC
- Bearbeitete Zeit: 18. Februar 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonChimeUserManagement`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "chime:ListAccounts",
        "chime:GetAccount",
        "chime:GetAccountSettings",
        "chime:UpdateAccountSettings",
        "chime:ListUsers",
        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroups",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Beschreibung: Verwaltete Richtlinie für Service Linked Role für Amazon Chime VoiceConnector

`AmazonChimeVoiceConnectorServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2019, 22:16 Uhr UTC
- Bearbeitete Zeit: 14. April 2023, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonChimeVoiceConnectorServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:UpdateDataRetention",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/ChimeVoiceConnector-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
```

```
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "chime:CreateMediaInsightsPipeline",
        "chime:GetMediaInsightsPipelineConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudDirectoryFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Cloud Directory Service.

`AmazonCloudDirectoryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudDirectoryFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Februar 2017, 00:41 UTC
- Zeit bearbeitet: 25. Februar 2017, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:*"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudDirectoryReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Cloud Directory Service.

`AmazonCloudDirectoryReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudDirectoryReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2017, 23:42 UTC
- Zeit bearbeitet: 28. Februar 2017, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudDirectoryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "clouddirectory:List*",
        "clouddirectory:Get*",
        "clouddirectory:LookupPolicy",
        "clouddirectory:BatchRead"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyFullAccess

Beschreibung: Bietet nur vollen Zugriff auf Amazon CloudWatch Eviently. Bietet auch Zugriff auf verwandte Amazon S3, Amazon SNS CloudWatch, Amazon und andere verwandte Dienste.

`AmazonCloudWatchEvidentlyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudWatchEvidentlyFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:10 Uhr UTC
- Bearbeitete Zeit: 29. November 2021, 15:10 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "evidently:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchRUMEvidentlyRole-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:TagResource",
        "cloudwatch:UnTagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Evidently-Alarm-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Evidently-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyReadOnlyAccess

Beschreibung: Bietet CloudWatch offensichtlich nur Lesezugriff auf Amazon

`AmazonCloudWatchEvidentlyReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudWatchEvidentlyReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:08 UTC
- Bearbeitete Zeit: 29. November 2021, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchEvidentlyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "evidently:GetExperiment",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchEvidentlyServiceRolePolicy

Beschreibung: Ermöglicht CloudWatch Evidently Service, die zugehörigen AWS Ressourcen im Namen des Kunden zu verwalten

`AmazonCloudWatchEvidentlyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 13. September 2022, 17:25 UTC
- Bearbeitete Zeit: 13. September 2022, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchEvidentlyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StartDeployment",
      "Resource" : [
        "arn:aws:appconfig:*:*:application/*",
        "arn:aws:appconfig:*:*:deploymentstrategy/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StartDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/configurationprofile/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/Owner" : "Evidently"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:TagResource",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    },
    {
      "Effect" : "Deny",
      "Action" : "appconfig:StopDeployment",
      "Resource" : "arn:aws:appconfig:*:*:application/*/environment/*/deployment/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/DeployedBy" : "Evidently"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "appconfig:ListDeployments",
      "Resource" : "arn:aws:appconfig:*:*:application/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMFullAccess

Beschreibung: Gewährt volle Zugriffsberechtigungen für den Amazon CloudWatch RUM-Service

`AmazonCloudWatchRUMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudWatchRUMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:46 Uhr UTC
- Bearbeitete Zeit: 29. November 2021, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetRole",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/rum.amazonaws.com/
AWSServiceRoleForRealUserMonitoring"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/RUM-Monitor*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cognito-identity:CreateIdentityPool",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:SetIdentityPoolRoles"
      ],
      "Resource" : "arn:aws:cognito-identity:*:*:identitypool/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*RUMService*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMReadOnlyAccess

Beschreibung: Gewährt Nur-Lese-Berechtigungen für den Amazon CloudWatch RUM-Service

`AmazonCloudWatchRUMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCloudWatchRUMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 15:43 Uhr UTC
- Bearbeitete Zeit: 12. Juni 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCloudWatchRUMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListRumMetricsDestinations",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetResourcePolicy",
        "rum:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:describeCanariesLastRun",
        "synthetics:describeCanaries"
      ],
      "Resource" : "arn:aws:synthetics:*:*:canary:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group::log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCloudWatchRUMServiceRolePolicy

Beschreibung: Erteilt Amazon CloudWatch RUM Service die Erlaubnis, Überwachungsdaten für andere relevante AWS Dienste zu veröffentlichen

`AmazonCloudWatchRUMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 23:17 UTC
- Bearbeitete Zeit: 22. Februar 2023, 20:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCloudWatchRUMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "RUM/CustomMetrics/*",
```

```
            "AWS/RUM"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeCatalyst

`AmazonCodeCatalystFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeCatalystFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2023, 16:50 UTC
- Bearbeitete Zeit: 20. April 2023, 16:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeCatalystResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:*",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCatalystAssociateIAMRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codecatalyst.amazonaws.com",
            "codecatalyst-runner.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon CodeCatalyst

`AmazonCodeCatalystReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeCatalystReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2023, 16:49 UTC
- Bearbeitete Zeit: 20. April 2023, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeCatalystReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecatalyst:Get*",
```

```
        "codecatalyst:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeCatalystSupportAccess

Beschreibung: Ermöglicht Amazon, AWS Support Fälle in Ihrem Namen CodeCatalyst zu erstellen, zu aktualisieren und zu lösen.

`AmazonCodeCatalystSupportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeCatalystSupportAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 12:34 UTC
- Bearbeitete Zeit: 20. April 2023, 12:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonCodeCatalystSupportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:SearchForCases",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:InitiateCallForCase",
        "support:InitiateChatForCase",
        "support:PutCaseAttributes",
        "support:RateCaseCommunication",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerAgentAccess

Beschreibung: Bietet Zugriff, der für den Amazon CodeGuru Profiler-Agent erforderlich ist.

`AmazonCodeGuruProfilerAgentAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruProfilerAgentAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Februar 2021, 22:11 UTC
- Bearbeitete Zeit: 5. Mai 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerAgentAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ConfigureAgent",
```

```
        "codeguru-profiler:CreateProfilingGroup",
        "codeguru-profiler:PostAgentProfile"
      ],
      "Resource" : "arn:aws:codeguru-profiler:*:*:profilingGroup/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruProfilerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 10:13 Uhr UTC
- Bearbeitete Zeit: 15. Juli 2020, 03:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru-profiler:*",
        "iam:ListRoles",
        "iam:ListUsers",
        "sns:ListTopics",
        "codeguru:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/*AWSServiceRoleForCodeGuruProfiler*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "codeguru-profiler.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruProfilerReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon CodeGuru Profiler.

`AmazonCodeGuruProfilerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruProfilerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 10:30 Uhr UTC
- Bearbeitete Zeit: 27. Juni 2020, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruProfilerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeguru:Get*",
        "codeguru-profiler:BatchGet*",
```

```
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerFullAccess

Beschreibung: Gewährt vollen Zugriff auf Amazon CodeGuru Reviewer und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonCodeGuruReviewerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruReviewerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 08:33 UTC
- Bearbeitete Zeit: 29. August 2020, 04:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:*",
        "codeguru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer"
    },
    {
      "Sid" : "CodeCommitAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:TagResource",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "codeguru-reviewer"
        }
      }
    },
    {
      "Sid" : "CodeConnectManagedRules",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:PassConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListRepositories",
            "ListOwners"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon CodeGuru Reviewer.

`AmazonCodeGuruReviewerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruReviewerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 08:48 UTC
- Bearbeitete Zeit: 29. August 2020, 04:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruReviewerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru:Get*",
        "codeguru-reviewer:List*",
```

```
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruReviewerServiceRolePolicy

Beschreibung: Eine servicebezogene Rolle, die Amazon CodeGuru Reviewer benötigt, um in Ihrem Namen auf Ressourcen zuzugreifen.

`AmazonCodeGuruReviewerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 05:31 Uhr UTC
- Bearbeitete Zeit: 27. November 2020, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCodeGuruReviewerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessCodeGuruReviewerEnabledRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetRepository",
        "codecommit:GetBranch",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetDifferences",
        "codecommit:GetPullRequest",
        "codecommit:ListPullRequests",
        "codecommit:PostCommentForPullRequest",
        "codecommit:GitPull",
        "codecommit:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/codeguru-reviewer" : "enabled"
        }
      }
    },
    {
      "Sid" : "AccessCodeGuruReviewerEnabledConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "codestar-connections:ProviderAction" : [
            "ListBranches",
            "GetBranch",
            "ListRepositories",
            "ListOwners",
            "ListPullRequests",
            "GetPullRequest",
            "ListPullRequestComments",
            "ListPullRequestCommits",
            "ListCommitFiles",
            "ListBranchCommits",
            "CreatePullRequestDiffComment",
            "GitPull"
          ]
        },
        "Null" : {
          "aws:ResourceTag/codeguru-reviewer" : "false"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsResourceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGuruS3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::codeguru-reviewer-*",
```

```
        "arn:aws:s3:::codeguru-reviewer-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruSecurityFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CodeGuru Security.

`AmazonCodeGuruSecurityFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruSecurityFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2023, 21:03 UTC
- Bearbeitete Zeit: 9. Mai 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCodeGuruSecurityScanAccess

Beschreibung: Bietet Zugriff, der für die Arbeit mit Amazon CodeGuru Security-Scans erforderlich ist.

`AmazonCodeGuruSecurityScanAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCodeGuruSecurityScanAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2023, 20:54 UTC

- Bearbeitete Zeit: 9. Mai 2023, 20:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCodeGuruSecurityScanAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonCodeGuruSecurityScanAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:CreateUploadUrl",
        "codeguru-security:GetScan",
        "codeguru-security:GetFindings"
      ],
      "Resource" : "arn:aws:codeguru-security:*:*:scans/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoDeveloperAuthenticatedIdentities

Beschreibung: Bietet Zugriff auf Amazon Cognito, um von Entwicklern authentifizierte Identitäten von Ihrem Authentifizierungs-Backend aus APIs zu unterstützen.

`AmazonCognitoDeveloperAuthenticatedIdentities`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonCognitoDeveloperAuthenticatedIdentities` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. März 2015, 17:22 Uhr UTC
- Bearbeitete Zeit: 24. März 2015, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoDeveloperAuthenticatedIdentities`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
```

```
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:MergeDeveloperIdentities",
        "cognito-identity:UnlinkDeveloperIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoIdpEmailServiceRolePolicy

Beschreibung: Ermöglicht dem Amazon Cognito User Pools-Service, Ihre SES-Identitäten für den E-Mail-Versand zu verwenden

`AmazonCognitoIdpEmailServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. März 2019, 21:32 Uhr UTC
- Bearbeitete Zeit: 21. März 2019, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpEmailServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:SendEmail",
        "ses:SendRawEmail"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ses:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoIdpServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon Cognito Cognito-Benutzerpools verwendet oder verwaltet werden

`AmazonCognitoIdpServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2020, 22:30 Uhr UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonCognitoIdpServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cognito-idp:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoPowerUser

Beschreibung: Bietet administrativen Zugriff auf bestehende Amazon Cognito Cognito-Ressourcen. Sie benötigen AWS-Konto Administratorrechte, um neue Cognito-Ressourcen zu erstellen.

`AmazonCognitoPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCognitoPowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. März 2015, 17:14 Uhr UTC
- Zeit bearbeitet: 27. Februar 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoPowerUser`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:*",
        "cognito-idp:*",
        "cognito-sync:*",
        "iam:ListRoles",
        "iam:ListOpenIdConnectProviders",
        "iam:GetRole",
        "iam:ListSAMLProviders",
        "iam:GetSAMLProvider",
        "kinesis:ListStreams",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "sns:GetSMSSandboxAccountStatus",
        "sns:ListPlatformApplications",
        "ses:ListIdentities",
        "ses:GetIdentityVerificationAttributes",
        "mobiletargeting:GetApps",
        "acm:ListCertificates",
        "sms-voice:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "cognito-idp.amazonaws.com",
            "email.cognito-idp.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdp*",
        "arn:aws:iam::*:role/aws-service-role/email.cognito-idp.amazonaws.com/
AWSServiceRoleForAmazonCognitoIdpEmail*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoReadOnly

Beschreibung: Bietet Lesezugriff auf Amazon Cognito Cognito-Ressourcen.

`AmazonCognitoReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonCognitoReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 24. März 2015, 17:06 UTC
- Bearbeitete Zeit: 1. August 2019, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-identity:Describe*",
        "cognito-identity:Get*",
        "cognito-identity:List*",
        "cognito-idp:Describe*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:List*",
        "cognito-idp:Get*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "iam:ListOpenIdConnectProviders",
        "iam:ListRoles",
        "sns:ListPlatformApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoUnAuthedIdentitiesSessionPolicy

Beschreibung: Diese Richtlinie definiert die Berechtigungen, die für nicht authentifizierte Identitäten für Cognito-Identitätspools zulässig sind. Diese Richtlinie ist nicht dafür vorgesehen, als eigenständige Berechtigungsrichtlinie verwendet zu werden. Sie dient als Schutzmaßnahme gegen übermäßig freizügige Richtlinien für Rollen in einem Identitätspool. Fügen Sie diese Richtlinie keiner Rolle hinzu, da Cognito Identity Service sie bei der Erstellung von Anmeldeinformationen automatisch als Richtlinie mit eingeschränktem Geltungsbereich einbezieht. Die Rechte für den temporären Zugriff auf andere AWS Ressourcen über den erweiterten Ablauf werden nun durch die Schnittmenge zwischen der Rolle, die mit der Identität des nicht authentifizierten Benutzers verknüpft ist, die von einem Dienst bereitgestellt wird, und den Rechten definiert, die in dieser verwalteten Richtlinie, die Cognito gehört, gewährt werden.

`AmazonCognitoUnAuthedIdentitiesSessionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonCognitoUnAuthedIdentitiesSessionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juli 2023, 23:04 UTC
- Bearbeitete Zeit: 1. November 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnAuthedIdentitiesSessionPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CognitoUnAuthedIdentitiesSessionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "rum:PutRumEvents",
        "sagemaker:InvokeEndpoint",
        "polly:*",
        "comprehend:*",
        "translate:*",
        "transcribe:*",
        "rekognition:*",
        "mobiletargeting:*",
        "firehose:*",
        "personalize:*",
        "geo:GetMap*",
        "geo:SearchPlaceIndex*",
        "geo:GetPlace",
        "geo:CalculateRoute*",
        "geo:*Geofence",
        "geo:*Geofences",
        "geo:*DevicePosition*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:GenerateDataKeyWithoutPlaintext"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonCognitoUnauthenticatedIdentities

Beschreibung: Diese Richtlinie definiert den Satz von Berechtigungen, die für nicht authentifizierte Identitäten für Cognito-Identitätspools zulässig sind. Dies muss nicht an Ihre Unauth-Rolle angehängt werden, da Cognito Identity Service es bei der Erstellung von Anmeldeinformationen automatisch als eingeschränkte Richtlinie einbezieht. Die Rechte für den temporären Zugriff auf andere AWS Ressourcen über den erweiterten Ablauf werden nun durch die Schnittmenge zwischen der Rolle, die mit der Identität des nicht authentifizierten Benutzers verknüpft ist, die von einem Dienst bereitgestellt wird, und den Rechten definiert, die in dieser verwalteten Richtlinie, die Cognito gehört, gewährt werden.

`AmazonCognitoUnauthenticatedIdentities`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonCognitoUnauthenticatedIdentities` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Februar 2023, 22:36 UTC
- Bearbeitete Zeit: 1. Februar 2023, 22:36 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonCognitoUnauthenticatedIdentities`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "rum:PutRumEvents",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnect_FullAccess

Beschreibung: Der Zweck dieser Richtlinie besteht darin, AWS Connect-Benutzern Berechtigungen zu gewähren, die für die Verwendung von Connect-Ressourcen erforderlich sind. Diese Richtlinie bietet vollen Zugriff auf AWS Connect-Ressourcen über die Connect Console und öffentlich APIs

`AmazonConnect_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonConnect_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 19:54 UTC
- Bearbeitete Zeit: 7. März 2023, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnect_FullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "connect:*",
        "ds:CreateAlias",
        "ds:AuthorizeApplication",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:UnauthorizeApplication",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "kinesis:DescribeStream",
```

```
        "kinesis:ListStreams",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lex:GetBots",
        "lex:ListBots",
        "lex:ListBotAliases",
        "logs:CreateLogGroup",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "lambda:ListFunctions",
        "ds:CheckAlias",
        "profile:ListAccountIntegrations",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:GetProfileObjectType",
        "profile:ListProfileObjectTypeTemplates"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:AddProfileKey",
        "profile:CreateDomain",
        "profile:CreateProfile",
        "profile:DeleteDomain",
        "profile:DeleteIntegration",
        "profile:DeleteProfile",
        "profile:DeleteProfileKey",
        "profile:DeleteProfileObject",
        "profile:DeleteProfileObjectType",
        "profile:GetIntegration",
        "profile:GetMatches",
        "profile:GetProfileObjectType",
        "profile:ListIntegrations",
        "profile:ListProfileObjects",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "profile:MergeProfiles",
        "profile:PutIntegration",
        "profile:PutProfileObject",
        "profile:PutProfileObjectType",
        "profile:SearchProfiles",
        "profile:TagResource",
```

```
        "profile:UntagResource",
        "profile:UpdateDomain",
        "profile:UpdateProfile"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::amazon-connect-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:connect/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "connect.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:DeleteServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "profile.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectCampaignsServiceLinkedRolePolicy

Beschreibung: Richtlinie für die mit dem Dienst Amazon Connect Campaigns verknüpfte Rolle

`AmazonConnectCampaignsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. September 2021, 20:54 UTC
- Bearbeitete Zeit: 03. Oktober 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectCampaignsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConnectCampaignAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:ListCampaigns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:BatchPutContact",
        "connect:StopContact",
        "connect:DescribeContactFlow",
        "connect:SendOutboundEmail"
      ],
      "Resource" : "arn:aws:connect:*:*:instance/*"
    },
    {
      "Sid" : "EventBridgeListRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EventBridgeManagedResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "connect-campaigns.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTargetsByRuleAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ConnectCampaignsRule*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectCampaignsEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:GetMessageTemplate",
        "wisdom:RenderMessageTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectCampaignsEnabled" : "True"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectReadOnlyAccess

Beschreibung: Erteilt die Berechtigung zum Anzeigen der Amazon Connect Connect-Instances in Ihrem AWS-Konto.

`AmazonConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Oktober 2018, 21:00 Uhr UTC
- Bearbeitete Zeit: 19. Juni 2024, 15:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "connect:Get*",
        "connect:Describe*",
        "connect:List*",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyConnectEmergencyAccess",
      "Effect" : "Deny",
      "Action" : "connect:AdminGetEmergencyAccessToken",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Connect, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AmazonConnectServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2018, 00:21 UTC
- Zeit bearbeitet: 18. November 2025, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v31 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AllowDeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect_*"
    },
    {
      "Sid" : "AllowS3ObjectForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*/*"
      ]
    },
    {
      "Sid" : "AllowGetBucketMetadataForConnectBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-connect-*"
      ]
    },
    {
      "Sid" : "AllowConnectLogGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/connect/*:*"
      ]
```

```
    },
    {
      "Sid" : "AllowListLexBotAccess",
      "Effect" : "Allow",
      "Action" : [
        "lex:ListBots",
        "lex:ListBotAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:SearchProfiles",
        "profile:CreateProfile",
        "profile:UpdateProfile",
        "profile:AddProfileKey",
        "profile:ListProfileObjectTypes",
        "profile:ListCalculatedAttributeDefinitions",
        "profile:ListCalculatedAttributesForProfile",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:GetIntegration",
        "profile:PutIntegration",
        "profile:DeleteIntegration",
        "profile:ListEventTriggers",
        "profile:ListSegmentDefinitions",
        "profile:ListProfileAttributeValues",
        "profile:CreateSegmentEstimate",
        "profile:GetSegmentEstimate",
        "profile:BatchGetProfile",
        "profile:BatchGetCalculatedAttributeForProfile",
        "profile:GetSegmentMembership",
        "profile:ListDomainLayouts",
        "profile:CreateUploadJob",
        "profile:ListUploadJobs",
        "profile:DetectProfileObjectType",
        "profile:GetSimilarProfiles",
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob",
        "profile:GetProfileRecommendations",
```

```
        "profile:GetProfileInsights",
        "profile:ListRecommenders"
      ],
      "Resource" : "arn:aws:profile:*:*:domains/amazon-connect-*"
    },
    {
      "Sid" : "AllowCustomerProfilesEventTriggerForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateEventTrigger",
        "profile:GetEventTrigger",
        "profile:UpdateEventTrigger",
        "profile:DeleteEventTrigger"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/event-triggers/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesDomainLayoutsForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateDomainLayout",
        "profile:UpdateDomainLayout",
        "profile:DeleteDomainLayout",
        "profile:GetDomainLayout"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/layouts/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationImportForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetUploadJob",
        "profile:GetUploadJobPath",
        "profile:StartUploadJob",
        "profile:StopUploadJob"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/upload-jobs/*"
      ]
    },
```

```
    {
      "Sid" : "AllowReadPermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjects",
        "profile:GetProfileObjectType",
        "profile:ListObjectTypeAttributes",
        "profile:ListObjectTypeAttributeValues"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilePredictiveInsights",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetRecommender",
        "profile:CreateRecommender",
        "profile:UpdateRecommender",
        "profile:DeleteRecommender",
        "profile:StopRecommender",
        "profile:StartRecommender"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/recommenders/*"
      ]
    },
    {
      "Sid" : "AllowReadPermissionForCustomerProfilesPersonalizeForRecommenderRecipes",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListRecommenderRecipes"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:*"
      ]
    },
    {
      "Sid" : "AllowListIntegrationForCustomerProfile",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListAccountIntegrations"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadForCustomerProfileObjectTemplates",
      "Effect" : "Allow",
      "Action" : [
        "profile:ListProfileObjectTypeTemplates",
        "profile:GetProfileObjectTypeTemplate"
      ],
      "Resource" : "arn:aws:profile:*:*:/templates*"
    },
    {
      "Sid" : "AllowAppIntegrationsForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "app-integrations:GetDataIntegration",
        "app-integrations:ListDataIntegrationAssociations",
        "app-integrations:CreateDataIntegrationSchedule",
        "app-integrations:StartDataIntegrationExecution",
        "app-integrations:ListDataIntegrationExecutions",
        "app-integrations:GetDataIntegrationExecution",
        "app-integrations:ListDataIntegrationSchedules",
        "app-integrations:UpdateDataIntegrationSchedule",
        "app-integrations:GetDataIntegrationSchedule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWisdomForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:CreateContent",
        "wisdom:DeleteContent",
        "wisdom:CreateKnowledgeBase",
        "wisdom:GetAssistant",
        "wisdom:GetKnowledgeBase",
        "wisdom:GetContent",
        "wisdom:GetRecommendations",
        "wisdom:GetSession",
```

```
        "wisdom:NotifyRecommendationsReceived",
        "wisdom:QueryAssistant",
        "wisdom:StartContentUpload",
        "wisdom:UpdateContent",
        "wisdom:UntagResource",
        "wisdom:TagResource",
        "wisdom:CreateSession",
        "wisdom:CreateQuickResponse",
        "wisdom:GetQuickResponse",
        "wisdom:SearchQuickResponses",
        "wisdom:StartImportJob",
        "wisdom:GetImportJob",
        "wisdom:ListImportJobs",
        "wisdom:ListQuickResponses",
        "wisdom:UpdateQuickResponse",
        "wisdom:DeleteQuickResponse",
        "wisdom:PutFeedback",
        "wisdom:ListContentAssociations",
        "wisdom:CreateMessageTemplate",
        "wisdom:UpdateMessageTemplate",
        "wisdom:UpdateMessageTemplateMetadata",
        "wisdom:GetMessageTemplate",
        "wisdom:DeleteMessageTemplate",
        "wisdom:ListMessageTemplates",
        "wisdom:SearchMessageTemplates",
        "wisdom:ActivateMessageTemplate",
        "wisdom:DeactivateMessageTemplate",
        "wisdom:CreateMessageTemplateVersion",
        "wisdom:ListMessageTemplateVersions",
        "wisdom:CreateMessageTemplateAttachment",
        "wisdom:DeleteMessageTemplateAttachment",
        "wisdom:RenderMessageTemplate",
        "wisdom:CreateAIAgent",
        "wisdom:CreateAIAgentVersion",
        "wisdom:DeleteAIAgent",
        "wisdom:DeleteAIAgentVersion",
        "wisdom:UpdateAIAgent",
        "wisdom:UpdateAssistantAIAgent",
        "wisdom:RemoveAssistantAIAgent",
        "wisdom:GetAIAgent",
        "wisdom:ListAIAgents",
        "wisdom:ListAIAgentVersions",
        "wisdom:CreateAIPrompt",
        "wisdom:CreateAIPromptVersion",
```

```
        "wisdom:DeleteAIPrompt",
        "wisdom:DeleteAIPromptVersion",
        "wisdom:UpdateAIPrompt",
        "wisdom:GetAIPrompt",
        "wisdom:ListAIPrompts",
        "wisdom:ListAIPromptVersions",
        "wisdom:CreateAIGuardrail",
        "wisdom:CreateAIGuardrailVersion",
        "wisdom:DeleteAIGuardrail",
        "wisdom:DeleteAIGuardrailVersion",
        "wisdom:UpdateAIGuardrail",
        "wisdom:GetAIGuardrail",
        "wisdom:ListAIGuardrails",
        "wisdom:ListAIGuardrailVersions",
        "wisdom:CreateAssistant",
        "wisdom:ListTagsForResource",
        "wisdom:SendMessage",
        "wisdom:GetNextMessage",
        "wisdom:ListMessages",
        "wisdom:Retrieve",
        "wisdom:ListAssistantAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowListOperationForWisdom",
      "Effect" : "Allow",
      "Action" : [
        "wisdom:ListAssistants",
        "wisdom:ListKnowledgeBases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCustomerProfilesCalculatedAttributesForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:GetCalculatedAttributeForProfile",
        "profile:CreateCalculatedAttributeDefinition",
```

```
        "profile:DeleteCalculatedAttributeDefinition",
        "profile:GetCalculatedAttributeDefinition",
        "profile:UpdateCalculatedAttributeDefinition"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/calculated-attributes/*"
      ]
    },
    {
      "Sid" : "AllowCustomerProfilesSegmentationForConnectDomain",
      "Effect" : "Allow",
      "Action" : [
        "profile:CreateSegmentDefinition",
        "profile:GetSegmentDefinition",
        "profile:DeleteSegmentDefinition",
        "profile:CreateSegmentSnapshot",
        "profile:GetSegmentSnapshot"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/segment-definitions/*"
      ]
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    },
    {
      "Sid" : "AllowSMSVoiceOperationsForConnect",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:SendTextMessage",
        "sms-voice:DescribePhoneNumbers"
      ],
      "Resource" : "arn:aws:sms-voice:*:*:phone-number/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowCognitoForConnectEnabledTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:ListUserPoolClients"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True"
        }
      }
    },
    {
      "Sid" : "AllowWritePermissionForCustomerProfileObjects",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObject"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/amazon-connect-*/object-types/*"
      ]
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorGetOperationForConnect",
      "Effect" : "Allow",
      "Action" : [
        "chime:GetVoiceConnector"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowChimeSDKVoiceConnectorListOperationForConnect",
      "Effect" : "Allow",
```

```
      "Action" : [
        "chime:ListVoiceConnectors"
      ],
      "Resource" : "arn:aws:chime:*:*:vc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionsForManagingReceiptRules",
      "Effect" : "Allow",
      "Action" : [
        "ses:DescribeReceiptRule",
        "ses:UpdateReceiptRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESPermissionForManagingConnectProvidedSESIdentity",
      "Effect" : "Allow",
      "Action" : [
        "ses:DeleteEmailIdentity"
      ],
      "Resource" : "arn:aws:ses:*:*:identity/*.email.connect.aws*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SESConfigurationSetPermissionsForSendingEmail",
      "Effect" : "Allow",
      "Action" : [
        "ses:SendRawEmail"
      ],
```

```
      "Resource" : "arn:aws:ses:*:*:configuration-set/configuration-set-for-connect-DO-
NOT-DELETE",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleToSESForReceiptRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonConnectEmailSESAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ses.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSocialMessagingOperations",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:SendWhatsAppMessage",
        "social-messaging:PostWhatsAppMessageMedia",
        "social-messaging:GetWhatsAppMessageMedia",
        "social-messaging:GetLinkedWhatsAppBusinessAccountPhoneNumber"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:phone-number-id/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWabas",
      "Effect" : "Allow",
      "Action" : [
```

```
        "social-messaging:ListLinkedWhatsAppBusinessAccounts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrievalOfWhatsAppTemplates",
      "Effect" : "Allow",
      "Action" : [
        "social-messaging:GetWhatsAppMessageTemplate",
        "social-messaging:ListWhatsAppMessageTemplates"
      ],
      "Resource" : "arn:aws:social-messaging:*:*:waba/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonConnectEnabled" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMobileTargetingOperationsForConnect",
      "Effect" : "Allow",
      "Action" : "mobiletargeting:SendMessages",
      "Resource" : "arn:aws:mobiletargeting:*:*:apps/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPollyActions",
      "Effect" : "Allow",
      "Action" : [
        "polly:ListLexicons",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectSynchronizationServiceRolePolicy

Beschreibung: Ermöglicht Amazon Connect, AWS Ressourcen in Ihrem Namen regionsübergreifend zu synchronisieren.

`AmazonConnectSynchronizationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. Oktober 2023, 22:38 UTC
- Bearbeitete Zeit: 21. November 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonConnectSynchronizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowConnectActions",
      "Effect" : "Allow",
      "Action" : [
        "connect:Create*",
        "connect:BatchCreate*",
        "connect:Update*",
        "connect:BatchUpdate*",
        "connect:Delete*",
        "connect:BatchDelete*",
        "connect:Describe*",
        "connect:BatchDescribe*",
        "connect:List*",
        "connect:Search*",
        "connect:Associate*",
        "connect:Disassociate*",
        "connect:Get*",
        "connect:BatchGet*",
        "connect:Import*",
        "connect:TagResource",
        "connect:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DisallowedConnectActions",
      "Effect" : "Deny",
      "Action" : [
        "connect:Start*",
        "connect:Stop*",
        "connect:Resume*",
        "connect:Suspend*",
        "connect:*Contact",
```

```
        "connect:SearchContacts",
        "connect:*ContactAttributes*",
        "connect:*RealtimeContact*",
        "connect:*AnalyticsData*",
        "connect:*MetricData*",
        "connect:*UserData*",
        "connect:*ContactEvaluation",
        "connect:*AttachedFile*",
        "connect:UpdateContactSchedule",
        "connect:UpdateContactRoutingData",
        "connect:ListContactReferences",
        "connect:CreateParticipant",
        "connect:CreatePersistentContactAssociation",
        "connect:CreateInstance",
        "connect:DeleteInstance",
        "connect:ListInstances",
        "connect:ReplicateInstance",
        "connect:GetFederationToken",
        "connect:ClaimPhoneNumber",
        "connect:ImportPhoneNumber",
        "connect:ReleasePhoneNumber",
        "connect:SearchAvailablePhoneNumbers",
        "connect:CreateTrafficDistributionGroup",
        "connect:DeleteTrafficDistributionGroup",
        "connect:GetTrafficDistribution",
        "connect:UpdateTrafficDistribution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricsForConnectNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Connect"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonConnectVoiceIDFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Connect Voice ID

`AmazonConnectVoiceIDFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonConnectVoiceIDFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. September 2021, 19:04 UTC
- Bearbeitete Zeit: 26. September 2021, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonConnectVoiceIDFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "voiceid:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneBedrockModelConsumptionPolicy

Beschreibung: Bietet Berechtigungen zur Nutzung von Amazon Bedrock-Modellen, einschließlich des Aufrufs eines Amazon Bedrock-Anwendungs-Inferenzprofils, das für eine bestimmte Amazon-Domain erstellt wurde. DataZone

`AmazonDataZoneBedrockModelConsumptionPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneBedrockModelConsumptionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. November 2024, 22:15 UTC
- Bearbeitete Zeit: 28. Mai 2025, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelConsumptionPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InvokeDomainInferenceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "ListFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockCreateSessionWithTagsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "bedrock:CreateSession",
        "bedrock:TagResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${datazone:domainId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:RequestTag/AmazonDataZoneDomain" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetSession",
        "bedrock:UpdateSession",
        "bedrock:DeleteSession",
        "bedrock:EndSession",
        "bedrock:CreateInvocation",
        "bedrock:ListInvocations",
        "bedrock:PutInvocationStep",
        "bedrock:GetInvocationStep",
        "bedrock:ListInvocationSteps",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "arn:aws:bedrock:*:*:session/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${datazone:userId}",
          "aws:ResourceTag/AmazonDataZoneDomain" : "${datazone:domainId}"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "",
          "aws:ResourceTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockListSessionsPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListSessions",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneBedrockModelManagementPolicy

Beschreibung: Bietet Berechtigungen zur Verwaltung des Zugriffs auf Amazon Bedrock-Modelle, einschließlich der Erstellung, Kennzeichnung und Löschung von Anwendungsinferenzprofilen.

`AmazonDataZoneBedrockModelManagementPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneBedrockModelManagementPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. November 2024, 22:14 UTC
- Bearbeitete Zeit: 12. November 2024, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneBedrockModelManagementPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfile",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingFoundationModels",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "CreateApplicationInferenceProfileUsingBedrockModels",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneDomainExecutionRolePolicy

Beschreibung: Standardrichtlinie für die DataZone DomainExecutionRole Servicerolle von Amazon. Diese Rolle wird von Amazon verwendet, DataZone um Daten in der DataZone Amazon-Domain zu katalogisieren, zu entdecken, zu verwalten, zu teilen und zu analysieren.

`AmazonDataZoneDomainExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneDomainExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. September 2023, 21:55 UTC

- Bearbeitete Zeit: 3. Dezember 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneDomainExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DomainExecutionRoleStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
```

```
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
```

```
            "datazone:GetGlossaryTerm",
            "datazone:GetGroupProfile",
            "datazone:GetLineageNode",
            "datazone:GetListing",
            "datazone:GetMetadataGenerationRun",
            "datazone:GetProject",
            "datazone:GetRule",
            "datazone:GetSubscription",
            "datazone:GetSubscriptionEligibility",
            "datazone:GetSubscriptionGrant",
            "datazone:GetSubscriptionRequestDetails",
            "datazone:GetSubscriptionTarget",
            "datazone:GetTimeSeriesDataPoint",
            "datazone:GetUserProfile",
            "datazone:ListAccountEnvironments",
            "datazone:ListAssetFilters",
            "datazone:ListAssetRevisions",
            "datazone:ListDataProductRevisions",
            "datazone:ListDataSourceRunActivities",
            "datazone:ListDataSourceRuns",
            "datazone:ListDataSources",
            "datazone:ListDomainUnitsForParent",
            "datazone:ListEntityOwners",
            "datazone:ListEnvironmentActions",
            "datazone:ListEnvironmentBlueprintConfigurationSummaries",
            "datazone:ListEnvironmentBlueprintConfigurations",
            "datazone:ListEnvironmentBlueprints",
            "datazone:ListEnvironmentProfiles",
            "datazone:ListEnvironments",
            "datazone:ListGroupsForUser",
            "datazone:ListLineageNodeHistory",
            "datazone:ListMetadataGenerationRuns",
            "datazone:ListNotifications",
            "datazone:ListPolicyGrants",
            "datazone:ListProjectMemberships",
            "datazone:ListProjects",
            "datazone:ListRules",
            "datazone:ListSubscriptionGrants",
            "datazone:ListSubscriptionRequests",
            "datazone:ListSubscriptionTargets",
            "datazone:ListSubscriptions",
            "datazone:ListTimeSeriesDataPoints",
            "datazone:ListWarehouseMetadata",
            "datazone:RejectPredictions",
```

```
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneEnvironmentRolePermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen für Umgebungen, um Datenanalyseaktionen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneEnvironmentRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneEnvironmentRolePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. September 2023, 23:38 UTC
- Bearbeitete Zeit: 17. November 2023, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneEnvironmentRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CreateGlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
```

```
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SameAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AnalyticsOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
```

```
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
```

```
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
```

```
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QueryOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryResultsStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsManagerOperationsWithTagKeys",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
```

```
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "*",
          "aws:ResourceTag/AmazonDataZoneProject" : "*"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid" : "DataZoneS3BucketLocation",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ListDataZoneS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
```

```
            "athena:ImportNotebook",
            "athena:ListDatabases",
            "athena:ListDataCatalogs",
            "athena:ListEngineVersions",
            "athena:ListNamedQueries",
            "athena:ListPreparedStatements",
            "athena:ListQueryExecutions",
            "athena:ListTableMetadata",
            "athena:ListTagsForResource",
            "athena:ListWorkGroups",
            "athena:StartCalculationExecution",
            "athena:StartQueryExecution",
            "athena:StartSession",
            "athena:StopCalculationExecution",
            "athena:StopQueryExecution",
            "athena:TerminateSession",
            "athena:UpdateNamedQuery",
            "athena:UpdateNotebook",
            "athena:UpdateNotebookMetadata",
            "athena:UpdatePreparedStatement",
            "ec2:CreateNetworkInterface",
            "ec2:CreateTags",
            "ec2:DeleteNetworkInterface",
            "ec2:DeleteTags",
            "ec2:Describe*",
            "glue:*DataQuality*",
            "glue:BatchCreatePartition",
            "glue:BatchDeleteConnection",
            "glue:BatchDeletePartition",
            "glue:BatchDeleteTable",
            "glue:BatchDeleteTableVersion",
            "glue:BatchGetJobs",
            "glue:BatchGetPartition",
            "glue:BatchGetWorkflows",
            "glue:BatchStopJobRun",
            "glue:BatchUpdatePartition",
            "glue:CreateBlueprint",
            "glue:CreateConnection",
            "glue:CreateCrawler",
            "glue:CreateDatabase",
            "glue:CreateJob",
            "glue:CreatePartition",
            "glue:CreatePartitionIndex",
            "glue:CreateTable",
```

```
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
```

```
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
```

```
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DataZone über die AWS-Managementkonsole sowie eingeschränkten Zugriff auf verwandte Dienste, die von Amazon benötigt werden.

`AmazonDataZoneFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:06 UTC
- Bearbeitete Zeit: 23. Juli 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
```

```
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "genai-studio-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
```

```
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneFullUserAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DataZone, ermöglicht jedoch nicht die Verwaltung von Domains, Benutzern oder zugehörigen Konten.

`AmazonDataZoneFullUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneFullUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 21:06 UTC
- Bearbeitete Zeit: 19. November 2024, 21:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneFullUserAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneUserOperations",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
```

```
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
```

```
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetIamPortalLoginUrl",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
```

```
        "datazone:PostTimeSeriesDataPoints",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareOperations",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShareAssociations",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneGlueManageAccessRolePolicy

Beschreibung: Die Richtlinie gewährt Amazon Berechtigungen, DataZone um die Veröffentlichung und den Zugriff auf Daten zu ermöglichen.

`AmazonDataZoneGlueManageAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneGlueManageAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:21 UTC
- Bearbeitete Zeit: 19. Juni 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneGlueManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "GlueTagDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringLikeIfExists" : {
          "aws:TagKeys" : "DataZoneDiscoverable_*"
        }
      }
    },
    {
      "Sid" : "GlueDataQuality",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListDataQualityResults",
        "glue:GetDataQualityResult"
      ],
      "Resource" : "arn:aws:glue:*:*:dataQualityRuleset/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueCrawler",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnection",
```

```
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTableDatabaseCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:CreateCatalog",
        "glue:CreateDatabase",
        "glue:DeleteCatalog",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGetTags",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
```

```
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:DeleteLakeFormationOptIn",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:UpdateDataCellsFilter",
        "glue:GetDatabase",
        "glue:GetTable",
        "organizations:DescribeOrganization",
        "ram:GetResourceShareInvitations",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LakeformationResourceFederatedSharing",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "lakeformation:GlueARN" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharing",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*"
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "GetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : "ram:GetResourceShares",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/datazone:projectId" : "proj-all"
        }
      }
    },
```

```
    {
      "Sid" : "GetRoleForDataZone",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*"
      ]
    },
    {
      "Sid" : "PassRoleForDataLocationRegistration",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerManageAccess*",
        "arn:aws:iam::*:role/datazone_usr_role*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCatalogEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CreateCatalogS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZonePortalFullAccessPolicy

Beschreibung: Bietet vollen Zugriff auf Amazon DataZone APIs

`AmazonDataZonePortalFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZonePortalFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. März 2023, 18:24 UTC
- Bearbeitete Zeit: 26. März 2023, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePortalFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "datazonecontrol:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZonePreviewConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Vorschauversion von Amazon DataZone über die AWS-Managementkonsole. Bietet auch ausgewählten Zugriff auf andere verwandte Dienste.

`AmazonDataZonePreviewConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZonePreviewConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. März 2023, 15:16 UTC
- Bearbeitete Zeit: 13. Juli 2023, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZonePreviewConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "datazonecontrol:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "glue:GetConnections",
        "glue:GetDatabase",
        "redshift:DescribeClusters",
        "ec2:DescribeSubnets",
        "secretsmanager:ListSecrets",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AmazonDataZone-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneBootstrapServicePolicy-
AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneServicePolicy-
AmazonDataZoneServiceRole"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneServiceRole*",
        "arn:aws:iam::*:role/AmazonDataZoneBootstrapRole*",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneBootstrapRole",
        "arn:aws:iam::*:role/AmazonDataZoneDomainExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonDataZoneDomainExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazonecontrol.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneProjectDeploymentPermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen, die es für die Bereitstellung von Datenanalyseprojekten verwendet. DataZone verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneProjectDeploymentPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneProjectDeploymentPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. März 2023, 02:54 UTC
- Bearbeitete Zeit: 4. April 2023, 02:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectDeploymentPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneProjectRolePermissionsBoundary"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:TagResource",
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:CreateLogGroup",
        "logs:TagLogGroup",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:*"
        },
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "kms:ScheduleKeyDeletion",
        "kms:DescribeKey",
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:Decrypt",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/datazone:projectId" : "proj-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "datazone:projectId"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:s3:::datazone*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/*datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*datazone*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:PutBucketLogging",
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*"
      ],
      "Resource" : "arn:aws:s3:::*datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:Get*",
        "athena:List*",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:Describe*",
        "ec2:Get*",
        "ec2:List*",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "logs:DeleteLogGroup",
        "logs:DeleteRetentionPolicy"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:PutKeyPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.logs",
            "com.amazonaws.*.s3",
            "com.amazonaws.*.glue",
            "com.amazonaws.*.athena"
          ]
        }
      }
    },
    {
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:TagResource",
        "cloudformation:GetTemplateSummary"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:GetEncryptionConfiguration",
        "s3:DeleteObject*",
        "s3:PutObject*",
        "s3:Abort*",
        "s3:DeleteBucket"
      ],
      "NotResource" : [
        "arn:aws:s3:::*datazone*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "kms:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Deny",
```

```
      "NotAction" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:GetParameter",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucketPolicy",
        "s3:CreateBucket",
        "s3:PutBucketAcl",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:DeleteBucket",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:CreatePolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicy",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeChangeSet",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplateSummary",
        "athena:*",
        "kms:*",
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabases",
        "glue:GetDatabase",
        "lambda:*",
        "ec2:*",
        "logs:*",
```

```
        "servicecatalog:CreateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:GetApplication",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy",
        "iam:UntagRole",
        "iam:PassRole",
        "iam:TagRole",
        "s3:GetBucket*",
        "s3:GetObject*",
        "s3:Abort*",
        "s3:GetEncryptionConfiguration",
        "s3:PutObject*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneProjectRolePermissionsBoundary

Beschreibung: Amazon DataZone erstellt IAM-Rollen für Projekte, um Datenanalyseaktionen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AmazonDataZoneProjectRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneProjectRolePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. März 2023, 02:51 UTC
- Bearbeitete Zeit: 21. März 2023, 02:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneProjectRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
```

```
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:List*",
        "s3:Get*",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "logs:*",
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
```

```
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGet*",
        "athena:List*",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:Get*",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:AcceptResourceShareInvitation",
        "ram:Get*",
        "ram:List*",
        "redshift:DescribeClusters",
        "redshift:JoinGroup",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift-data:*",
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares",
```

```
        "redshift:AssociateDataShareConsumer",
        "tag:GetResources",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "glue:CreateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateDataQualityRuleset",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateWorkflow",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:List*",
```

```
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/datazone:projectId" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:SearchTables",
        "glue:List*",
        "glue:Get*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
```

```
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:DeleteResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "NotAction" : [
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:DeleteObjectVersion",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutObjectRetention",
        "s3:DeleteObject",
        "kms:List*",
        "kms:Get*",
        "kms:Describe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:GenerateDataKey",
        "ec2:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "logs:*",
        "athena:*",
        "glue:BatchGet*",
        "glue:Get*",
```

```
        "glue:SearchTables",
        "glue:List*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:PutResourcePolicy",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:UpdatePartition",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
```

```
        "glue:UpdateConnection",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "lakeformation:GetDataAccess",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:GrantPermissions",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "ram:*",
        "redshift:*",
        "redshift-data:*",
        "tag:GetResources",
        "iam:List*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:PassRole",
        "sqlworkbench:*",
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneRedshiftGlueProvisioningPolicy

Beschreibung: Amazon DataZone ist ein Datenverwaltungsservice, mit dem Sie Ihre Daten katalogisieren, ermitteln, verwalten, teilen und analysieren können. Mit Amazon DataZone können Sie Ihre Daten über Konten und unterstützte Regionen hinweg teilen und darauf zugreifen. Amazon DataZone vereinfacht Ihre Erfahrung mit allen AWS Services, einschließlich, aber nicht beschränkt auf Amazon Redshift, Amazon Athena, AWS Glue und AWS Lake Formation.

`AmazonDataZoneRedshiftGlueProvisioningPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneRedshiftGlueProvisioningPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2023, 20:19 UTC
- Bearbeitete Zeit: 23. Oktober 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneRedshiftGlueProvisioningPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackCreationForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneCFStackManagementForEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:ListPermissions",
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "athena:GetWorkGroup",
        "logs:DescribeLogGroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift:DescribeClusters",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AmazonDataZoneEnvironmentGlueDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentAthenaResourceCreation",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource",
        "iam:TagRole",
        "iam:TagPolicy",
        "logs:TagLogGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupCreation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentLogGroupManagement",
      "Action" : [
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:datazone-*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentIAMPolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentS3ValidationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSDecryptPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : "AmazonDataZoneEnvironment"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ListSchemas",
        "redshift-data:ExecuteStatement"
      ],
      "Resource" : [
```

```
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "DescribeStatementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSecretValuePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneRedshiftManageAccessRolePolicy

Beschreibung: Diese Richtlinie erteilt Amazon die DataZone Erlaubnis, Amazon Redshift Redshift-Daten im Katalog zu veröffentlichen. Es gibt Amazon auch die DataZone Erlaubnis, Zugriff auf

veröffentlichte Amazon Redshift- oder Amazon Redshift Serverless-Assets im Katalog zu gewähren oder den Zugriff zu widerrufen.

`AmazonDataZoneRedshiftManageAccessRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneRedshiftManageAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. September 2023, 20:15 UTC
- Bearbeitete Zeit: 7. März 2025, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDataZoneRedshiftManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "redshiftDataScopeDownPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
```

```
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift:*:*:cluster:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "listSecretsPermission",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "getWorkgroupPermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetWorkgroup",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteWorkgroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "getNamespacePermission",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetNamespace",
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "createAndDeleteNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:DeleteNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "redshiftDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "dataSharesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare",
        "redshift:DescribeDataShares"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "associateDataShareConsumerPermission",
      "Effect" : "Allow",
      "Action" : "redshift:AssociateDataShareConsumer",
      "Resource" : "arn:aws:redshift:*:*:datashare:*/datazone*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

Beschreibung: Die AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary Richtlinie ist die Liste der Berechtigungen, die für eine Ausführungsrolle zulässig sind, die in einer von Amazon DataZone bereitgestellten SageMaker Umgebung erstellt wurde.

`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:01 UTC
- Bearbeitete Zeit: 17. November 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Sid" : "AllowSageMakerProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile",
        "sagemaker:UpdateUserProfile",
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:*/*"
    },
    {
      "Sid" : "AllowLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsForDomainResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
```

```
        "arn:aws:sagemaker:*:*:user-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateApp",
            "CreateSpace",
            "CreateUserProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListSpaces",
        "sagemaker:ListUserProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
```

```
          "sagemaker:SpaceSharingType" : [
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AllowAWSServiceActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*",
        "datazone:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
```

```
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "groundtruthlabeling:*",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowRAMInvitation",
      "Effect" : "Allow",
      "Action" : "ram:AcceptResourceShareInvitation",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "dzd*"
        }
      }
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker*",
        "arn:aws:ecr:*:*:repository/datazone*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
```

```
        "arn:aws:codecommit:*:*:*SageMaker*",
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
```

```
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
```

```
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::Sagemaker-DataZone*",
        "arn:aws:s3:::DataZone-Sagemaker*",
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::amazon-datazone*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "states.amazonaws.com",
            "lakeformation.amazonaws.com",
            "events.amazonaws.com",
            "sagemaker.amazonaws.com",
            "forecast.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CrossAccountKmsOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KmsOperationsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
```

```
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:domain/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:ListJobs",
```

```
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:GetDatabases",
        "glue:GetTables",
        "glue:GetTable",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:ListSchemas",
        "glue:BatchGetJobs",
        "glue:GetConnection",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AllowGlueActionsWithEnvironmentTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:ListSchemas",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "AllowGlueDefaultAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGet*",
        "glue:Get*",
        "glue:SearchTables",
        "glue:List*",
        "glue:RunStatement"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:connection/dz-sm-*",
        "arn:aws:glue:*:*:session/*"
      ]
    },
    {
      "Sid" : "AllowRedshiftClusterActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowCreateClusterUser",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateClusterUser"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*"
      ]
    },
    {
      "Sid" : "AllowCreateSecretActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*",
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
```

```
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventBridgeRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEMR",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSOAction",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DenyNotAction",
      "Effect" : "Deny",
      "NotAction" : [
        "sagemaker:*",
        "sagemaker-geospatial:*",
        "sqlworkbench:*",
        "datazone:*",
        "forecast:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
```

```
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage",
        "ecr:StartImageScan",
        "ecr:TagResource",
        "ecr:UntagResource",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListClusters",
        "events:PutRule",
        "events:DescribeRule",
        "events:PutTargets",
        "events:TagResource",
        "events:ListTagsForResource",
        "fsx:DescribeFileSystems",
        "glue:SearchTables",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:StopCrawler",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:UpdateCrawler",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:StartCrawler",
        "glue:ResetJobBookmark",
        "glue:UpdateJob",
```

```
        "glue:StartWorkflowRun",
        "glue:StopCrawlerSchedule",
        "glue:ResumeWorkflowRun",
        "glue:DeleteCrawler",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:BatchGet*",
        "glue:UpdateCrawlerSchedule",
        "glue:DeleteConnection",
        "glue:UpdateConnection",
        "glue:Get*",
        "glue:BatchDeleteConnection",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:CreateWorkflow",
        "glue:*DataQuality*",
        "glue:List*",
        "glue:CreateSession",
        "glue:RunStatement",
        "glue:BatchCreatePartition",
        "glue:CreateDatabase",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:BatchUpdatePartition",
        "glue:BatchDeletePartition",
        "glue:UpdateTable",
        "glue:DeleteTableVersion",
        "glue:DeleteTable",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchDeleteTable",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:UpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "groundtruthlabeling:*",
```

```
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:RetireGrant",
        "lakeformation:GetDataAccess",
        "lambda:ListFunctions",
        "lambda:InvokeFunction",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:UpdateLogDelivery",
        "ram:AcceptResourceShareInvitation",
        "rds:DescribeDBInstances",
        "redshift:CreateClusterUser",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:DescribeClusters",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:GetBucketAcl",
```

```
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCors",
        "s3:PutBucketCors",
        "s3:DeleteObjectVersion",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:TagResource",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine",
        "tag:GetResources",
        "sso:CreateApplicationAssignment",
        "sso:AssociateProfile"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerManageAccessRolePolicy

Beschreibung: Die AmazonDataZoneSageMakerManageAccessRolePolicy Richtlinie gewährt Amazon DataZone die erforderlichen Berechtigungen, um Benutzern Zugriff auf verschiedene Ressourcen in der SageMaker Umgebung zu gewähren.

`AmazonDataZoneSageMakerManageAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneSageMakerManageAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:34 UTC
- Bearbeitete Zeit: 21. November 2024, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerManageAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:ListModelPackages",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:ListTags",
        "sagemaker:DescribeDomain",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:shared-with:*"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "AmazonSageMakerModelPackageGroupPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:DeleteModelPackageGroupPolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerRAMResourcePolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:PutResourcePolicy",
        "sagemaker:GetResourcePolicy",
        "sagemaker:DeleteResourcePolicy"
      ],
      "Resource" : [
        "arn:*:sagemaker:*:*:feature-group/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerRAMTagResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "AmazonSageMakerRAMDeleteResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:*:ram:*:*:resource-share/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerRAMCreateResourceSharePermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "sagemaker:*"
          ]
        },
        "Null" : {
          "aws:RequestTag/AwsDataZoneDomainId" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerS3BucketPolicyPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
```

```
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-datazone*",
        "arn:aws:s3:::SageMaker-DataZone*",
        "arn:aws:s3:::datazone-sagemaker*",
        "arn:aws:s3:::DataZone-SageMaker*",
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:DeleteRepositoryPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerKMSGrantPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDataZoneSageMakerProvisioningRolePolicy

Beschreibung: Die AmazonDataZoneSageMakerProvisioningRolePolicy Richtlinie gewährt Amazon DataZone die für die Zusammenarbeit mit Amazon SageMaker erforderlichen Berechtigungen.

`AmazonDataZoneSageMakerProvisioningRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDataZoneSageMakerProvisioningRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2024, 23:32 UTC
- Zeit bearbeitet: 9. Januar 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDataZoneSageMakerProvisioningRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false",
          "aws:RequestTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSageMakerStudio",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteDomain"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneEnvironment"
          ]
        },
        "Null" : {
          "aws:TagKeys" : "false",
```

```
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com"
          ],
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateEnvironmentRole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ],
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToManageEnvironmentRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentParameterValidation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "sagemaker:ListDomains"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentKMSKeyValidation",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "false"
        }
      }
    },
    {
      "Sid" : "AmazonDataZoneEnvironmentGluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection",
        "glue:GetConnection"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
        "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Abhängigkeiten der Konsolen-Benutzeroberfläche

`AmazonDetectiveFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDetectiveFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 30. April 2020, 17:57 UTC
- Bearbeitete Zeit: 17. Mai 2023, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings"
      ],
      "Resource" : "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveInvestigatorAccess

Beschreibung: Bietet Ermittlern Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Benutzeroberflächenabhängigkeiten der Konsole. Diese Richtlinie gewährt die Erlaubnis, Detective zu Ermittlungszwecken zu nutzen, und gewährt eingeschränkten Schreibzugriff auf Guardduty.

`AmazonDetectiveInvestigatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDetectiveInvestigatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2023, 15:24 UTC

- Bearbeitete Zeit: 27. November 2023, 03:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveInvestigatorAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DetectivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
```

```
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityHub:GetFindings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveMemberAccess

Beschreibung: Bietet Mitgliedern Zugriff auf den Amazon Detective Service und bereichsspezifischen Zugriff auf die Abhängigkeiten der Konsolen-Benutzeroberfläche.

`AmazonDetectiveMemberAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDetectiveMemberAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2023, 15:16 UTC
- Bearbeitete Zeit: 17. Januar 2023, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveMemberAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
```

```
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveOrganizationsAccess

Beschreibung: Bietet Organizations Zugriff auf die Verwaltung des delegierten Administrators für Amazon Detective und bereichsspezifischen Zugriff auf die Benutzeroberflächenabhängigkeiten der Konsole. Dadurch wird auch die Erlaubnis erteilt, eine dienstbezogene Rolle für Detective zu erstellen.

`AmazonDetectiveOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDetectiveOrganizationsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. März 2023, 15:20 UTC
- Bearbeitete Zeit: 2. März 2023, 15:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDetectiveOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDetectiveServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Detective, Serviceanrufe in Ihrem Namen zu tätigen

`AmazonDetectiveServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2021, 19:47 UTC
- Bearbeitete Zeit: 18. November 2021, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDetectiveServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruConsoleFullAccess

Beschreibung: Die Richtlinie gewährt vollen Zugriff auf die DevOps Guru-Konsole.

`AmazonDevOpsGuruConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDevOpsGuruConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Dezember 2021, 18:43 UTC
- Bearbeitete Zeit: 25. August 2022, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PerformanceInsightsMetricsDataAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "pi:GetResourceMetrics",
        "pi:DescribeDimensionKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DevOps Guru.

`AmazonDevOpsGuruFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDevOpsGuruFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:38 UTC
- Zeit bearbeitet: 25. August 2022, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsListTopicsAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnsTopicOperations",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOps-Guru-*"
    },
    {
      "Sid" : "DevOpsGuruSlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DevOpsGuruSlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruOrganizationsAccess

Beschreibung: Stellen Sie Zugriff bereit, um Amazon DevOps Guru innerhalb einer Organisation zu aktivieren und zu verwalten.

`AmazonDevOpsGuruOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDevOpsGuruOrganizationsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2021, 23:50 UTC
- Bearbeitete Zeit: 15. November 2021, 23:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:SearchOrganizationInsights"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "OrganizationsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "arn:aws:organizations::*:"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "devops-guru.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf die Amazon DevOps Guru Console.

`AmazonDevOpsGuruReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDevOpsGuruReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:34 UTC
- Zeit bearbeitet: 25. August 2022, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDevOpsGuruReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DevOpsGuruReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:DescribeAccountHealth",
```

```
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudFormationListStacksAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
    },
    {
      "Sid" : "CloudWatchGetMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeDBInstancesAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsFilterLogEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDevOpsGuruServiceRolePolicy

Beschreibung: Eine servicebezogene Rolle, die Amazon benötigt, DevOpsGuru um auf Ihre Ressourcen zugreifen zu können.

`AmazonDevOpsGuruServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2020, 10:24 Uhr UTC
- Bearbeitete Zeit: 10. Januar 2023, 14:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDevOpsGuruServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudtrail:LookupEvents",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListDashboards",
        "cloudwatch:GetDashboard",
```

```
        "cloudformation:GetTemplate",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
```

```
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketWebsite",
        "s3:GetIntelligentTieringConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListStorageLensConfigurations",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutTargetsOnASpecificRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
    },
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAddTagsToOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreateManagedRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowAccessManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
    },
    {
      "Sid" : "AllowOtherOperationsOnManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "devops-guru.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowTagBasedFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DevOps-Guru-Analysis" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAPIGatewayGetIntegrations",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/??????????",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSCloudWatchLogsRole

Beschreibung: Ermöglicht den Zugriff auf das Hochladen von DMS-Replikationsprotokollen in Cloudwatch-Protokolle im Kundenkonto.

`AmazonDMSCloudWatchLogsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDMSCloudWatchLogsRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. Januar 2016, 23:44 UTC
- Bearbeitete Zeit: 23. Mai 2023, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeOnAllLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid" : "AllowCreationOfDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    },
    {
      "Sid" : "AllowUploadOfLogEventsToDmsLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-
serverless-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSRedshiftS3Role

Beschreibung: Ermöglicht den Zugriff auf die Verwaltung von S3-Einstellungen für Redshift-Endpunkte für DMS.

`AmazonDMSRedshiftS3Role`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonDMSRedshiftS3Role` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2016, 17:05 Uhr UTC
- Bearbeitete Zeit: 8. Juli 2019, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::dms-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDMSVPCManagementRole

Beschreibung: Bietet Zugriff auf die Verwaltung von VPC-Einstellungen für AWS verwaltete Kundenkonfigurationen

`AmazonDMSVPCManagementRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDMSVPCManagementRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. November 2015, 16:33 UTC
- Bearbeitete Zeit: 25. Juli 2024, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDB-ElasticServiceRolePolicy

Beschreibung: Ermöglicht Amazon DocumentDB-Elastic, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonDocDB-ElasticServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2022, 14:17 UTC

- Zeit bearbeitet: 30. November 2022, 14:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonDocDB-ElasticServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Elastic"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon DocumentDB mit MongoDB-Kompatibilität mithilfe von. AWS-Managementkonsole Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von EC2 Amazon-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten von Schlüsseln auf Amazon KMS sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

`AmazonDocDBConsoleFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonDocDBConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:37 UTC
- Bearbeitete Zeit: 11. Februar 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbSids",
      "Effect" : "Allow",
```

```
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction",
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeAccountAttributes",
```

```
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DependencySids",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DocdbSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DocdbElasticSLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBElasticFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DocumentDB Elastic Clusters und andere erforderliche Berechtigungen für dessen Abhängigkeiten EC2, einschließlich KMS CloudWatch und IAM. SecretsManager

`AmazonDocDBElasticFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDocDBElasticFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Juni 2023, 13:51 UTC
- Bearbeitete Zeit: 11. Februar 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DocdbElasticSid",
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:CreateCluster",
        "docdb-elastic:UpdateCluster",
        "docdb-elastic:GetCluster",
        "docdb-elastic:DeleteCluster",
        "docdb-elastic:ListClusters",
        "docdb-elastic:CreateClusterSnapshot",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:DeleteClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:RestoreClusterFromSnapshot",
        "docdb-elastic:TagResource",
        "docdb-elastic:UntagResource",
        "docdb-elastic:ListTagsForResource",
        "docdb-elastic:CopyClusterSnapshot",
        "docdb-elastic:StartCluster",
        "docdb-elastic:StopCluster",
        "docdb-elastic:GetPendingMaintenanceAction",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ApplyPendingMaintenanceAction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Sid",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KMSSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ],
          "aws:ResourceTag/DocDBElasticFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "KMSGrantSid",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/DocDBElasticFullAccess" : "*",
          "kms:ViaService" : [
            "docdb-elastic.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "SecretManagerSid",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/DocDBElasticFullAccess" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "docdb-elastic.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudwatchSid",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "SLRSid",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/docdb-elastic.amazonaws.com/
AWSServiceRoleForDocDB-Elastic",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "docdb-elastic.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBElasticReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DoCDB-Elastic und Metriken. CloudWatch

`AmazonDocDBElasticReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonDocDBElasticReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juni 2023, 14:37 UTC

- Bearbeitete Zeit: 21. Juni 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBElasticReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "docdb-elastic:ListClusters",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos sowie vollen Zugriff auf Amazon RDS und Amazon Neptune gewährt.

`AmazonDocDBFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonDocDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:21 UTC
- Bearbeitete Zeit: 9. Januar 2019, 20:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBCluster",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBInstance",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
```

```
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
```

```
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDocDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DocumentDB mit MongoDB-Kompatibilität. Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon RDS- und Amazon Neptune Neptune-Ressourcen gewährt.

`AmazonDocDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDocDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Januar 2019, 20:30 Uhr UTC
- Bearbeitungszeit: 9. Januar 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDocDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
```

```
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
```

```
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDRSVPCManagement

Beschreibung: Bietet Zugriff auf die Verwaltung der VPC-Einstellungen für von Amazon verwaltete Kundenkonfigurationen

`AmazonDRSVPCManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDRSVPCManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. September 2015, 00:09 Uhr UTC
- Zeit bearbeitet: 2. September 2015, 00:09 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDRSVPCManagement`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon DynamoDB über die. AWS-Managementkonsole

`AmazonDynamoDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDynamoDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 29. Januar 2021, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "dynamodb:*",
        "dax:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
```

```
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes",
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetFunctionConfiguration",
        "lambda:DeleteFunction",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:DeleteGroup",
        "resource-groups:CreateGroup",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com",
            "application-autoscaling.amazonaws.com.cn",
            "dax.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBFullAccess_v2

Beschreibung: Bietet vollen Zugriff auf Amazon DynamoDB

`AmazonDynamoDBFullAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDynamoDBFullAccess_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Mai 2025, 14:52 UTC
- Bearbeitete Zeit: 22. Mai 2025, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DDBAndDAXFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:*",
        "dax:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaIntegration",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DaxSNSIntegration",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchMonitoring",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListKinesisResources",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEC2ResourcesForDaxClusterCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchInsightsRules",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetInsightRuleReport",
```

```
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Sid" : "ServiceRoleCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.dynamodb.amazonaws.com",
            "dax.amazonaws.com",
            "dynamodb.application-autoscaling.amazonaws.com",
            "contributorinsights.dynamodb.amazonaws.com",
            "kinesisreplication.dynamodb.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBFullAccesswithDataPipeline

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https://docs.aws.amazon.com/amazondynamodb/ latest/developerguide/DynamoDBPipeline.html. Provides full access to Amazon DynamoDB including Export/Import Verwenden von AWS Data Pipeline über die AWS-Managementkonsole.

`AmazonDynamoDBFullAccesswithDataPipeline`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDynamoDBFullAccesswithDataPipeline` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 12. November 2015, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccesswithDataPipeline`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:*",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsole"
    },
    {
      "Action" : [
        "lambda:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleTriggers"
    },
    {
      "Action" : [
        "datapipeline:*",
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "DDBConsoleImportExport"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRolePolicy",
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Sid" : "IAMEDPRoles"
    },
    {
      "Action" : [
        "ec2:CreateTags",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "EMR"
    },
    {
      "Action" : [
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:Put*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Sid" : "S3"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonDynamoDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon DynamoDB über die. AWS-Managementkonsole

`AmazonDynamoDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonDynamoDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 18. November 2024, 17:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonDynamoDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralReadOnlyAccess",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "dynamodb:BatchGetItem",
        "dynamodb:Describe*",
        "dynamodb:List*",
        "dynamodb:GetAbacStatus",
        "dynamodb:GetItem",
        "dynamodb:GetResourcePolicy",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dax:Describe*",
        "dax:List*",
        "dax:GetItem",
        "dax:BatchGetItem",
        "dax:Query",
        "dax:Scan",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "iam:GetRole",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "lambda:ListFunctions",
        "lambda:ListEventSourceMappings",
        "lambda:GetFunctionConfiguration",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupQuery",
        "tag:GetResources",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CCIAccess",
      "Action" : "cloudwatch:GetInsightRuleReport",
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEBSCSIDriverPolicy

Beschreibung: IAM-Richtlinie, die es dem CSI-Treiberdienstkonto ermöglicht, Anrufe an verwandte Dienste zu tätigen, z. B. in EC2 Ihrem Namen.

`AmazonEBSCSIDriverPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEBSCSIDriverPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. April 2022, 17:24 UTC
- Bearbeitete Zeit: 17. November 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyVolumes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/vol-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot",
            "CopyVolumes"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:CopyVolumes"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/kubernetes.io/created-for/pvc/name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ebs.csi.aws.com/cluster" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/CSIVolumeSnapshotName" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ebs.csi.aws.com/cluster" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryFullAccess

Beschreibung: Bietet administrativen Zugriff auf Amazon ECR-Ressourcen

`AmazonEC2ContainerRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Dezember 2015, 17:06 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:04 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "replication.ecr.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryPowerUser

Beschreibung: Bietet vollen Zugriff auf Amazon EC2 Container Registry-Repositorys, erlaubt jedoch weder das Löschen von Repositorys noch Richtlinienänderungen.

`AmazonEC2ContainerRegistryPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerRegistryPowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 21. Dezember 2015, 17:05 Uhr UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPowerUser`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryPullOnly

Beschreibung: Ermöglicht den Zugriff auf das Abrufen von Images aus Amazon EC2 Container Registry-Repositorys.

`AmazonEC2ContainerRegistryPullOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerRegistryPullOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Oktober 2024, 16:58 UTC
- Bearbeitungszeit: 4. Oktober 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryPullOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchImportUpstreamImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerRegistryReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EC2 Container Registry-Repositorys.

`AmazonEC2ContainerRegistryReadOnly`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerRegistryReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Dezember 2015, 17:04 UTC
- Bearbeitete Zeit: 10. Dezember 2019, 20:56 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:GetLifecyclePolicy",
        "ecr:GetLifecyclePolicyPreview",
        "ecr:ListTagsForResource",
        "ecr:DescribeImageScanFindings"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceAutoscaleRole

Beschreibung: Richtlinie zur Aktivierung von Task Autoscaling für Amazon EC2 Container Service

`AmazonEC2ContainerServiceAutoscaleRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerServiceAutoscaleRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Mai 2016, 23:25 Uhr UTC
- Bearbeitete Zeit: 5. Februar 2018, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceAutoscaleRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceEventsRole

Beschreibung: Richtlinie zur Aktivierung von CloudWatch Ereignissen für EC2 Container Service

`AmazonEC2ContainerServiceEventsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerServiceEventsRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. Mai 2017, 16:51 UTC
- Bearbeitete Zeit: 06. März 2023, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceEventsRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:RunTask"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RunTask"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceforEC2Role

Beschreibung: Standardrichtlinie für die EC2 Amazon-Rolle für Amazon EC2 Container Service.

`AmazonEC2ContainerServiceforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerServiceforEC2Role` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. März 2015, 18:45 Uhr UTC
- Zeit bearbeitet: 4. August 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ecs:CreateCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:DiscoverPollEndpoint",
        "ecs:Poll",
        "ecs:RegisterContainerInstance",
        "ecs:StartTelemetrySession",
        "ecs:UpdateContainerInstancesState",
        "ecs:Submit*",
```

```
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterContainerInstance"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*",
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ContainerServiceRole

Beschreibung: Standardrichtlinie für die Amazon ECS-Servicerolle.

`AmazonEC2ContainerServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ContainerServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 16:14 UTC
- Bearbeitete Zeit: 11. August 2016, 13:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:Describe*",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
```

```
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2FullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EC2 über die AWS-Managementkonsole.

`AmazonEC2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 27. November 2018, 02:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "ec2:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "ec2scheduled.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "transitgateway.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ImageReferencesAccessPolicy

Beschreibung: Bietet Lesezugriff, um bei der Verwendung alle unterstützten Ressourcentypen nach relevanten Daten zu durchsuchen. DescribeImageReferences

`AmazonEC2ImageReferencesAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ImageReferencesAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. August 2025, 19:19 UTC
- Zeit bearbeitet: 26. August 2025, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ImageReferencesAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:DescribeImageReferences",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeParameters",
        "ssm:GetParameters",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:GetContainerRecipe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ec2-images.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2ReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon EC2 über die AWS-Managementkonsole.

`AmazonEC2ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 27. Dezember 2024, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:Describe*",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforAWSCodeDeploy

Beschreibung: Ermöglicht EC2 den Zugriff auf den S3-Bucket, um die Revision herunterzuladen. Diese Rolle wird vom CodeDeploy Agenten auf EC2 Instances benötigt.

`AmazonEC2RoleforAWSCodeDeploy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2RoleforAWSCodeDeploy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2015, 18:10 Uhr UTC
- Bearbeitete Zeit: 20. März 2017, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeploy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforAWSCodeDeployLimited

Beschreibung: Bietet EC2 eingeschränkten Zugriff auf den S3-Bucket zum Herunterladen der Revision. Diese Rolle wird vom CodeDeploy Agenten auf EC2 Instances benötigt.

`AmazonEC2RoleforAWSCodeDeployLimited`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2RoleforAWSCodeDeployLimited` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. August 2020, 17:55 Uhr UTC
- Bearbeitete Zeit: 20. Januar 2022, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforAWSCodeDeployLimited`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforDataPipelineRole

Beschreibung: Standardrichtlinie für die EC2 Servicerolle Amazon Role for Data Pipeline.

`AmazonEC2RoleforDataPipelineRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2RoleforDataPipelineRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 22. Februar 2016, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforDataPipelineRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "datapipeline:*",
        "dynamodb:*",
```

```
        "ec2:Describe*",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListInstance*",
        "elasticmapreduce:ModifyInstanceGroups",
        "rds:Describe*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RoleforSSM

Beschreibung: Diese Richtlinie wird bald veraltet sein. Bitte verwenden Sie SSMManaged InstanceCore die Amazon-Richtlinien, um die Kernfunktionen des AWS Systems Manager Manager-Service für EC2 Instances zu aktivieren. Weitere Informationen finden Sie unter https:// docs.aws.amazon.com/systems-manager/ latest/userguide/setup -instance-profile.html

`AmazonEC2RoleforSSM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2RoleforSSM` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. Mai 2015, 17:48 Uhr UTC
- Bearbeitete Zeit: 24. Januar 2019, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2RoleforSSM`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetEncryptionConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2RolePolicyForLaunchWizard

Beschreibung: Verwaltete Richtlinie für die LaunchWizard Amazon-Servicerolle für EC2

`AmazonEC2RolePolicyForLaunchWizard`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2RolePolicyForLaunchWizard` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 08:05 UTC
- Bearbeitete Zeit: 25. September 2024, 22:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEC2RolePolicyForLaunchWizard`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardResourceGroupID" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceRoute"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeRouteTables",
        "ec2:ModifyInstanceAttribute",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricData",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "LaunchWizardResourceGroupID",
            "LaunchWizardApplicationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:GetBucketLocation",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*",
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:Create*",
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "cloudformation:DescribeStackResources",
        "cloudformation:SignalResource",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "LaunchWizardResourceGroupID"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:PutItem",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "dynamodb:Scan",
        "s3:ListBucket",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteTable",
        "dynamodb:CreateTable",
        "s3:GetObject",
        "dynamodb:DescribeTable",
        "s3:GetBucketLocation",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:dynamodb:*:*:table/LaunchWizard*",
        "arn:aws:sqs:*:*:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/LaunchWizardApplicationType" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackint",
```

```
        "arn:aws:ssm:*:*:document/AWSSAP-InstallBackintForAWSBackup"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:ListTagsForResource",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2SpotFleetAutoscaleRole

Beschreibung: Richtlinie zur Aktivierung von Autoscaling für Amazon EC2 Spot Fleet

`AmazonEC2SpotFleetAutoscaleRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2SpotFleetAutoscaleRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. August 2016, 18:27 UTC
- Bearbeitete Zeit: 18. Februar 2019, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetAutoscaleRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEC2SpotFleetTaggingRole

Beschreibung: Ermöglicht EC2 Spot Fleet, Spot-Instances in Ihrem Namen anzufordern, zu beenden und zu kennzeichnen.

`AmazonEC2SpotFleetTaggingRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEC2SpotFleetTaggingRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. Juni 2017, 18:19 Uhr UTC

- Bearbeitete Zeit: 23. April 2020, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEC2SpotFleetTaggingRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
```

```
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECS_FullAccess

Beschreibung: Bietet administrativen Zugriff auf Amazon ECS-Ressourcen und ermöglicht ECS-Funktionen durch Zugriff auf andere AWS Serviceressourcen VPCs, einschließlich Auto Scaling Scaling-Gruppen und CloudFormation Stacks.

`AmazonECS_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECS_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2017, 21:36 UTC
- Bearbeitete Zeit: 13. August 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECS_FullAccess`

Version der Richtlinie

Richtlinienversion: v21 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSIntegrationsManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
```

```
        "appmesh:ListMeshes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:Describe*",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
        "cloudformation:UpdateStack",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ContinueDeployment",
        "codedeploy:CreateApplication",
        "codedeploy:CreateDeployment",
        "codedeploy:CreateDeploymentGroup",
        "codedeploy:GetApplication",
        "codedeploy:GetApplicationRevision",
        "codedeploy:GetDeployment",
        "codedeploy:GetDeploymentConfig",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:GetDeploymentTarget",
        "codedeploy:ListApplicationRevisions",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codedeploy:ListDeploymentGroups",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "codedeploy:RegisterApplicationRevision",
        "codedeploy:StopDeployment",
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateInternetGateway",
```

```
        "ec2:CreateLaunchTemplate",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RequestSpotFleet",
        "ec2:RunInstances",
        "ecs:*",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget",
        "events:ListTargetsByRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "fsx:DescribeFileSystems",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRoles",
        "lambda:ListFunctions",
        "logs:CreateLogGroup",
```

```
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "servicediscovery:CreatePrivateDnsNamespace",
        "servicediscovery:CreateService",
        "servicediscovery:DeleteService",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetOperation",
        "servicediscovery:GetService",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:UpdateService",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/aws/service/ecs*"
    },
    {
      "Sid" : "ManagedCloudformationResourcesCleanupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteInternetGateway",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "EC2ContainerService-*"
        }
      }
    },
    {
      "Sid" : "TasksPassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ecs-tasks.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InfrastructurePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInfrastructureRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstancePassRolePolicy",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
```

```
        ]
      }
    }
  },
  {
    "Sid" : "AutoScalingPassRolePolicy",
    "Action" : "iam:PassRole",
    "Effect" : "Allow",
    "Resource" : [
      "arn:aws:iam::*:role/ecsAutoscaleRole*"
    ],
    "Condition" : {
      "StringLike" : {
        "iam:PassedToService" : [
          "application-autoscaling.amazonaws.com",
          "application-autoscaling.amazonaws.com.cn"
        ]
      }
    }
  },
  {
    "Sid" : "ServiceLinkedRoleCreationPolicy",
    "Effect" : "Allow",
    "Action" : "iam:CreateServiceLinkedRole",
    "Resource" : "*",
    "Condition" : {
      "StringLike" : {
        "iam:AWSServiceName" : [
          "ecs.amazonaws.com",
          "autoscaling.amazonaws.com",
          "ecs.application-autoscaling.amazonaws.com",
          "spot.amazonaws.com",
          "spotfleet.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid" : "ELBTaggingPolicy",
    "Effect" : "Allow",
    "Action" : [
      "elasticloadbalancing:AddTags"
    ],
    "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateTargetGroup",
            "CreateRule",
            "CreateListener",
            "CreateLoadBalancer"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSComputeServiceRolePolicy

Beschreibung: Richtlinie, die es Amazon ECS Compute ermöglicht, Ihre EC2 Instances und zugehörige Ressourcen als Teil von ECS-verwalteten Instances zu verwalten

`AmazonECSComputeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. März 2025, 17:37 UTC

- Bearbeitete Zeit: 28. März 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSComputeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissionsForInstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeFleets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteManagedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TerminateManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRoleforExpressGatewayServices

Beschreibung: Diese Berechtigungen ermöglichen Amazon ECS die automatische Bereitstellung und Verwaltung der für Express Gateway Services erforderlichen Infrastrukturkomponenten, einschließlich Lastenausgleich, Sicherheitsgruppen, SSL-Zertifikate und Auto Scaling-Konfigurationen.

`AmazonECSInfrastructureRoleforExpressGatewayServices`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRoleforExpressGatewayServices` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. November 2025, 20:34 UTC
- Bearbeitete Zeit: 15. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRoleforExpressGatewayServices`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ServiceLinkedRoleCreateOperations",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ecs.application-autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ELBOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateRule",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:ModifyRule",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeleteListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateELBResources",
```

```
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:AddTags",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
            "CreateListener",
            "CreateRule",
            "CreateTargetGroup"
          ]
        }
      }
    },
    {
      "Sid" : "BlanketAllowCreateSecurityGroupsInVPCs",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateSecurityGroupResourcesWithTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ModifySecurityGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateEC2Resources",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress",
            "AuthorizeSecurityGroupEgress"
          ]
        }
      }
    },
    {
      "Sid" : "CertificateOperations",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate",
        "acm:AddTagsToCertificate",
```

```
        "acm:DeleteCertificate",
        "acm:DescribeCertificate"
      ],
      "Resource" : [
        "arn:aws:acm:*:*:certificate/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:TagResource",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingPolicyOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "ecs"
        }
      }
```

```
    },
    {
      "Sid" : "ApplicationAutoscalingReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*"
      ]
    },
    {
      "Sid" : "CloudWatchAlarmCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchAlarmOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsCreateOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForLoadBalancers

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Verwaltung von Load Balancern im Zusammenhang mit ECS-Workloads in Ihrem Namen erforderlich sind.

`AmazonECSInfrastructureRolePolicyForLoadBalancers`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRolePolicyForLoadBalancers` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Juli 2025, 16:37 UTC
- Bearbeitete Zeit: 25. Juli 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForLoadBalancers`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ELBReadOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*"
    },
    {
      "Sid" : "ALBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/app/*/*/*"
      ]
    },
    {
      "Sid" : "NLBModifyListeners",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyListener",
      "Resource" : [
```

```
        "arn:aws:elasticloadbalancing:*:*:listener/net/*/*/*"
      ]
    },
    {
      "Sid" : "ALBModifyRules",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:ModifyRule",
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/*/*/*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForManagedInstances

Beschreibung: Bietet ECS-Zugriff zum Erstellen und Verwalten EC2 verwalteter Ressourcen

`AmazonECSInfrastructureRolePolicyForManagedInstances`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRolePolicyForManagedInstances` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. September 2025, 18:04 UTC
- Bearbeitete Zeit: 15. Dezember 2025, 22:49 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForManagedInstances`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateLaunchTemplateForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateLaunchTemplateVersionsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ProvisionEC2InstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateFleetForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "RunInstancesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForECSManagedLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesForSupportingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "TagOnCreateEC2ResourcesForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "PassInstanceRoleForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/ecsInstanceRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEC2Spot",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ]
    },
    {
      "Sid" : "DescribeEC2ResourcesManagedByECS",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerS

Beschreibung: Bietet Administratorzugriff auf Private Certificate Authority, AWS Secrets Manager und andere, die für die Verwaltung der TLS-Funktionen von ECS Service Connect in Ihrem Namen AWS-Services erforderlich sind.

`AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Januar 2024, 20:08 UTC
- Bearbeitete Zeit: 13. November 2025, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "TagOnCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : [
            "arn:aws:ecs:*:*:service/*/*",
            "arn:aws:ecs:*:*:task-set/*/*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RotateTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecretVersionStage"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "ecs-sc",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DescribeTLSCertificateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecs-sc!*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthority",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificate",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManagePrivateCertificateAuthorityForIssuingEndEntityCertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true",
          "acm-pca:TemplateArn" : "arn:aws:acm-pca:::template/EndEntityCertificate/V1"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForVolumes

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Verwaltung von Volumes im Zusammenhang mit ECS-Workloads in Ihrem Namen erforderlich sind.

`AmazonECSInfrastructureRolePolicyForVolumes`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRolePolicyForVolumes` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. Januar 2024, 22:56 UTC
- Bearbeitete Zeit: 28. Mai 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSInfrastructureRolePolicyForVolumes`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "CreateEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSManagedVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Sid" : "TagOnCreateVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVolume",
          "aws:RequestTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumesForLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DescribeInstancesForAttachingVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageEBSVolumeLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ManageVolumeAttachmentsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DeleteEBSManagedVolume",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:ResourceTag/AmazonECSCreated" : "arn:aws:ecs:*:*:task/*"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonECSManaged" : "true"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInfrastructureRolePolicyForVpcLattice

Beschreibung: Bietet Zugriff auf andere AWS Serviceressourcen, die für die Verwaltung der VPC Lattice-Funktion in ECS-Workloads in Ihrem Namen erforderlich sind.

`AmazonECSInfrastructureRolePolicyForVpcLattice`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonECSInfrastructureRolePolicyForVpcLattice` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 20:02 UTC
- Bearbeitete Zeit: 15. November 2024, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInfrastructureRolePolicyForVpcLattice`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManagedVpcLatticeTargetRegistration",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:RegisterTargets",
        "vpc-lattice:DeregisterTargets"
      ],
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeVpcLatticeTargetGroup",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:GetTargetGroup",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "ListVpcLatticeTargets",
      "Effect" : "Allow",
      "Action" : "vpc-lattice:ListTargets",
      "Resource" : [
        "arn:aws:vpc-lattice:*:*:targetgroup/*"
      ]
    },
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSInstanceRolePolicyForManagedInstances

Beschreibung: Standardrichtlinie für die Amazon ECS-Instance-Rolle für Amazon ECS Managed Instances.

`AmazonECSInstanceRolePolicyForManagedInstances`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSInstanceRolePolicyForManagedInstances` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. September 2025, 23:49 UTC
- Bearbeitete Zeit: 26. September 2025, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonECSInstanceRolePolicyForManagedInstances`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAgentDiscoverPollEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DiscoverPollEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSAgentRegisterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterContainerInstance"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    },
    {
      "Sid" : "ECSAgentPollPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentTelemetryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StartTelemetrySession",
```

```
        "ecs:PutSystemLogEvents"
      ],
      "Resource" : "arn:aws:ecs:*:*:container-instance/*"
    },
    {
      "Sid" : "ECSAgentStateChangePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:SubmitAttachmentStateChanges",
        "ecs:SubmitTaskStateChange"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSServiceRolePolicy

Beschreibung: Richtlinie, um Amazon ECS die Verwaltung Ihres Clusters zu ermöglichen.

`AmazonECSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 14. Oktober 2017, 01:18 Uhr UTC
- Zeit bearbeitet: 20. November 2025, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonECSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSTaskManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:AssociateTrunkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:Describe*",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateTrunkInterface",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:Describe*",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:Get*",
        "route53:List*",
```

```
        "route53:UpdateHealthCheck",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:UpdateInstanceCustomHealthStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:PutLifecycleHook",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:RecordLifecycleActionHeartbeat"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "autoscaling:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "AutoScalingPlanManagement",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling-plans:CreateScalingPlan",
        "autoscaling-plans:DeleteScalingPlan",
        "autoscaling-plans:DescribeScalingPlans",
```

```
        "autoscaling-plans:DescribeScalingPlanResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/ecs-managed-*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CWAlarmManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ECSTagging",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
```

```
    },
    {
      "Sid" : "CWLogGroupManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*"
    },
    {
      "Sid" : "CWLogStreamManagement",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/*:log-stream:*"
    },
    {
      "Sid" : "ExecuteCommandSessionManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExecuteCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*",
        "arn:aws:ssm:*:*:document/AmazonECS-ExecuteInteractiveCommand"
      ]
    },
    {
      "Sid" : "CloudMapResourceCreation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicediscovery:CreateHttpNamespace",
        "servicediscovery:CreateService"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonECSManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CloudMapResourceTagging",
      "Effect" : "Allow",
      "Action" : "servicediscovery:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonECSManaged" : "*"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDeletion",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DeleteService"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CloudMapResourceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudMapResourceAttributeManagement",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:UpdateServiceAttributes"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonECSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForInstanceEventWindows",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceEventWindows"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonECSTaskExecutionRolePolicy

Beschreibung: Bietet Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon ECS-Aufgaben erforderlich sind

`AmazonECSTaskExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonECSTaskExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2017, 18:48 Uhr UTC
- Zeit bearbeitet: 16. November 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEFSCSIDriverPolicy

Beschreibung: Bietet Verwaltungszugriff auf EFS-Ressourcen und Lesezugriff auf EC2

`AmazonEFSCSIDriverPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEFSCSIDriverPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. Juli 2023, 20:10 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEFSCSIDriverPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateAccessPoint",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateAccessPoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowTagNewAccessPoints",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticfilesystem:CreateAction" : "CreateAccessPoint"
        },
```

```
        "Null" : {
          "aws:RequestTag/efs.csi.aws.com/cluster" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "efs.csi.aws.com/cluster"
        }
      }
    },
    {
      "Sid" : "AllowDeleteAccessPoint",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:DeleteAccessPoint",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/efs.csi.aws.com/cluster" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKS_CNI_Policy

Beschreibung: Diese Richtlinie gewährt dem Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) die erforderlichen Berechtigungen, um die IP-Adresskonfiguration auf Ihren EKS-Worker-Knoten zu ändern. Dieser Berechtigungssatz ermöglicht es dem CNI, Elastic Network Interfaces in Ihrem Namen aufzulisten, zu beschreiben und zu ändern. Weitere Informationen zum AWS VPC CNI Plugin finden Sie hier: 8s https://github.com/aws/ amazon-vpc-cni-k

`AmazonEKS_CNI_Policy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonEKS_CNI_Policy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:07 UTC
- Bearbeitete Zeit: 4. März 2024, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSCNIPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSCNIPolicyENITag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSBlockStoragePolicy

Beschreibung: Mit der EKS-Clusterrolle verknüpfte Richtlinie, die Berechtigungen zur Verwaltung der Blockspeicherressourcen des Clusters gewährt.

`AmazonEKSBlockStoragePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSBlockStoragePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 30. Oktober 2024, 20:18 UTC
- Bearbeitete Zeit: 30. Oktober 2024, 20:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSBlockStoragePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:ModifyVolume",
        "ec2:EnableFastSnapshotRestores"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
```

```
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "kubernetes.io/created-for/*",
            "Name",
            "KubernetesCluster"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "CSIVolumeSnapshotName",
            "ebs.csi.eks.amazonaws.com/cluster",
            "kubernetes.io/cluster/*",
            "Name"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSClusterPolicy

Beschreibung: Diese Richtlinie gewährt Kubernetes die erforderlichen Berechtigungen, um Ressourcen in Ihrem Namen zu verwalten. Kubernetes benötigt Ec2: CreateTags -Berechtigungen, um identifizierende Informationen auf EC2 Ressourcen zu platzieren, einschließlich, aber nicht beschränkt auf Instances, Sicherheitsgruppen und Elastic Network Interfaces.

`AmazonEKSClusterPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonEKSClusterPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:06 UTC
- Bearbeitete Zeit: 17. April 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSClusterPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSClusterPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:UpdateAutoScalingGroup",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteRoute",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DetachVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyVolume",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstanceTopology",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
```

```
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEKSClusterPolicySLRCreate",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonEKSClusterPolicyENIDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "amazon-vpc-cni"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSComputePolicy

Beschreibung: Mit der EKS-Clusterrolle verknüpfte Richtlinie, die Berechtigungen zur Verwaltung der Rechenressourcen des Clusters gewährt.

`AmazonEKSComputePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSComputePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. November 2024, 21:46 UTC
- Bearbeitete Zeit: 20. Juni 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSComputePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-node-class-name" : "*",
          "aws:RequestTag/eks:kubernetes-node-pool-name" : "*"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-node-class-name",
```

```
            "eks:kubernetes-node-pool-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSConnectorServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht Amazon EKS die Verwaltung von AWS Ressourcen für den EKS-Connector.

`AmazonEKSConnectorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. September 2021, 20:31 UTC
- Bearbeitete Zeit: 15. Oktober 2025, 22:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSConnectorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccessSSMService",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation",
        "ssm:DescribeInstanceInformation",
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConnectorAgentStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:ssm:*::document/AmazonEKS-ExecuteNonInteractiveCommand"
      ]
    },
    {
      "Sid" : "ConnectorAgentDeregister",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "PassAnyRoleToSsm",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutManagedEventRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.ssm"
        }
      }
    },
    {
      "Sid" : "PutManagedEventTarget",
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "eks-connector.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "OpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSDashboardConsoleReadOnly

Beschreibung: Bietet Lesezugriff zur Anzeige des Dashboards in der Amazon EKS-Konsole. Das Dashboard aggregiert Informationen über mehrere Cluster und zugehörige Ressourcen mithilfe von AWS Organizations.

`AmazonEKSDashboardConsoleReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSDashboardConsoleReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2025, 17:22 UTC
- Bearbeitete Zeit: 19. Juni 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSDashboardConsoleReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEKSDashboardReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListDashboardData",
        "eks:ListDashboardResources",
        "eks:DescribeClusterVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonOrganizationsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSDashboardServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es dem Amazon EKS-Dashboard, auf unternehmensweite Informationen zuzugreifen und diese anzuzeigen. Die Richtlinie ermöglicht es dem EKS-Dashboard-Dienst, Informationen über die Struktur und Konten Ihrer AWS Organizations zu sammeln.

`AmazonEKSDashboardServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Mai 2025, 19:07 UTC

- Bearbeitete Zeit: 8. Mai 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSDashboardServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsReadActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSFargatePodExecutionRolePolicy

Beschreibung: Bietet Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon EKS-Pods auf AWS Fargate erforderlich sind

`AmazonEKSFargatePodExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSFargatePodExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2019, 04:34 UTC
- Bearbeitete Zeit: 22. November 2019, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSFargatePodExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
```

```
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSForFargateServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Amazon EKS die erforderlichen Berechtigungen zur Ausführung von Fargate-Aufgaben.

`AmazonEKSForFargateServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. November 2019, 04:36 Uhr UTC
- Bearbeitete Zeit: 22. November 2019, 04:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSForFargateServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSLoadBalancingPolicy

Beschreibung: Mit der EKS-Clusterrolle verknüpfte Richtlinie, die Berechtigungen zur Verwaltung der Lastenausgleichsressourcen des Clusters gewährt.

`AmazonEKSLoadBalancingPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSLoadBalancingPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Oktober 2024, 20:18 UTC
- Bearbeitete Zeit: 09. Januar 2025, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLoadBalancingPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:CreateTargetGroup",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:CreateRule",
        "ec2:CreateSecurityGroup"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:targetgroup/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group-rule/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer",
```

```
            "CreateTargetGroup",
            "CreateListener",
            "CreateRule"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:SetIpAddressType",
        "elasticloadbalancing:SetSecurityGroups",
        "elasticloadbalancing:SetSubnets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:ModifyListenerAttributes",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "wafv2:AssociateWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:DeleteProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "shield:TagResource"
      ],
      "Resource" : "arn:aws:shield::*:protection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "ingress.eks.amazonaws.com/stack",
            "ingress.eks.amazonaws.com/resource",
            "service.eks.amazonaws.com/stack",
            "service.eks.amazonaws.com/resource"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPoolClient",
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "elasticloadbalancing:SetWebAcl",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSLocalOutpostClusterPolicy

Beschreibung: Diese Richtlinie gewährt den Kontrollebeneninstanzen des lokalen EKS-Clusters, die in Ihrem Konto ausgeführt werden, Berechtigungen, um Ressourcen in Ihrem Namen zu verwalten.

`AmazonEKSLocalOutpostClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSLocalOutpostClusterPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. August 2022, 21:56 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSLocalOutpostClusterPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeAvailabilityZones",
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:DescribeInstanceProperties",
        "ssm:DescribeDocumentParameters",
        "ssm:ListInstanceAssociations",
        "ssm:RegisterManagedInstance",
        "ssm:UpdateInstanceInformation",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:PutComplianceItems",
        "ssm:PutInventory",
        "ecr-public:GetAuthorizationToken",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/eks/*",
        "arn:aws:ecr:*:*:repository/bottlerocket-admin",
        "arn:aws:ecr:*:*:repository/bottlerocket-control-eks",
        "arn:aws:ecr:*:*:repository/diagnostics-collector-eks",
        "arn:aws:ecr:*:*:repository/kubelet-config-updater"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
```

```
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSLocalOutpostServiceRolePolicy

Beschreibung: Ermöglicht Amazon EKS Local, AWS Dienste in Ihrem Namen anzurufen.

`AmazonEKSLocalOutpostServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. August 2022, 21:53 UTC
- Bearbeitete Zeit: 26. Juni 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSLocalOutpostServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribePlacementGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup",
            "RunInstances"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*",
            "eks*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DeleteSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:DescribeSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:eks-local.cluster.x-k8s.io/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-local-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/eks-local:controlplane-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*::document/AmazonEKS-ControlPlaneInstanceProxy"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ResumeSession",
```

```
        "ssm:TerminateSession"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSMCPReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon EKS MCP Service. Diese Richtlinie gewährt die Erlaubnis, nur schreibgeschützte Tools im EKS MCP-Service zu verwenden, die zur Beobachtbarkeit, Fehlerbehebung, zum Abrufen von EKS-Ressourceninformationen und zum Abrufen von EKS-optimierten Vorschlägen bestimmt sind.

`AmazonEKSMCPReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonEKSMCPReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2025, 17:19 Uhr UTC
- Zeit bearbeitet: 20. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSMCPReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:ListClusters",
        "eks:DescribeNodegroup",
        "eks:ListNodegroups",
        "eks:DescribeAddon",
        "eks:ListAddons",
        "eks:DescribeAccessEntry",
        "eks:ListAccessEntries",
        "eks:DescribeInsight",
        "eks:ListInsights",
        "eks:AccessKubernetesApi"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks-mcp:InvokeMcp",
        "eks-mcp:CallReadOnlyTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSNetworkingPolicy

Beschreibung: Mit der EKS-Clusterrolle verknüpfte Richtlinie, die Berechtigungen zur Verwaltung der Netzwerkressourcen des Clusters gewährt.

`AmazonEKSNetworkingPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSNetworkingPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Oktober 2024, 22:34 UTC
- Bearbeitete Zeit: 28. Oktober 2024, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSNetworkingPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        },
        "StringLike" : {
          "aws:RequestTag/eks:kubernetes-cni-node-name" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "eks:eks-cluster-name",
            "eks:kubernetes-cni-node-name"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "${aws:PrincipalTag/eks:eks-cluster-
name}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSServicePolicy

Beschreibung: Diese Richtlinie ermöglicht es Amazon Elastic Container Service for Kubernetes, die für den Betrieb von EKS-Clustern erforderlichen Ressourcen zu erstellen und zu verwalten.

`AmazonEKSServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSServicePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:08 UTC
- Bearbeitete Zeit: 14. Oktober 2024, 21:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSServicePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "iam:ListAttachedRolePolicies",
        "eks:UpdateClusterVersion",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "eks.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle ist erforderlich, damit Amazon EKS AWS Services in Ihrem Namen anrufen kann.

`AmazonEKSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Februar 2020, 20:10 UTC
- Zeit bearbeitet: 22. Oktober 2025, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEKSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
```

```
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeListenerAttributes",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTrustStores",
        "iam:ListAttachedRolePolicies",
        "pricing:GetProducts",
        "shield:GetSubscriptionState",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/Name" : "eks-cluster-sg*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/Name" : "eks-cluster-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "route53:AssociateVPCWithHostedZone",
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/eks/*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AWS/EKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry",
        "eks:DeleteAccessEntry"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "STANDARD"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/eks.amazonaws.com/
AWSServiceRoleForAmazonEKS"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/${aws:PrincipalAccount}/
AWSServiceRoleForAmazonEKS/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : [
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputePolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSComputeClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSNetworkingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSLoadBalancingPolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSLoadBalancingClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSBlockStoragePolicy",
            "arn:aws:eks::aws:cluster-access-policy/
AmazonEKSBlockStorageClusterPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSHybridPolicy",
            "arn:aws:eks::aws:cluster-access-policy/AmazonEKSEventPolicy"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "eks:DescribeAccessEntry",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "eks:accessEntryType" : "EC2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/EKS*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.ec2",
            "aws.health"
          ]
        },
        "StringEquals" : {
          "events:ManagedBy" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "events:PutTargets",
```

```
      "Resource" : "arn:aws:events:*:*:rule/EKS*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : [
            "eks.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteRule",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeleteTargetGroup",
        "ec2:DeleteSecurityGroup",
        "shield:DescribeProtection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/eks:eks-cluster-name" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSVPCResourceController

Beschreibung: Richtlinie, die vom VPC Resource Controller zur Verwaltung von ENI und IPs für Worker-Knoten verwendet wird.

`AmazonEKSVPCResourceController`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSVPCResourceController` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. August 2020, 00:55 UTC
- Zeit bearbeitet: 12. August 2020, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSVPCResourceController`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "ec2:ResourceTag/eks:eni:owner" : "eks-vpc-resource-controller"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSWorkerNodeMinimalPolicy

Beschreibung: Diese Richtlinie ermöglicht es Amazon EKS-Worker-Knoten, sich mit Amazon EKS-Clustern zu verbinden.

`AmazonEKSWorkerNodeMinimalPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSWorkerNodeMinimalPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Oktober 2024, 20:03 UTC
- Bearbeitete Zeit: 2. Oktober 2024, 20:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodeMinimalPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEKSWorkerNodePolicy

Beschreibung: Diese Richtlinie ermöglicht es Amazon EKS-Worker-Knoten, sich mit Amazon EKS-Clustern zu verbinden.

`AmazonEKSWorkerNodePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEKSWorkerNodePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2018, 21:09 UTC
- Bearbeitete Zeit: 27. November 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkerNodePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "eks-auth:AssumeRoleForPodIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon ElastiCache über die AWS-Managementkonsole.

`AmazonElastiCacheFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElastiCacheFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 28. November 2023, 03:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : "elasticache:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/elasticache.amazonaws.com/
AWSServiceRoleForElastiCache",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticache.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpoints",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToEc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToAutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScalingActivities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListLogDeliveryStreams",
      "Effect" : "Allow",
      "Action" : [
```

```
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToOutposts",
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElastiCacheReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon ElastiCache über die AWS-Managementkonsole.

`AmazonElastiCacheReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElastiCacheReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElastiCacheReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticache:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicFullAccess

Beschreibung: Bietet administrativen Zugriff auf öffentliche Ressourcen von Amazon ECR

`AmazonElasticContainerRegistryPublicFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticContainerRegistryPublicFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 17:25 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 17:25 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:*",
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicPowerUser

Beschreibung: Bietet vollen Zugriff auf öffentliche Amazon ECR-Repositorys, erlaubt jedoch nicht das Löschen von Repositorys oder Richtlinienänderungen.

`AmazonElasticContainerRegistryPublicPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticContainerRegistryPublicPowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:16 UTC
- Zeit bearbeitet: 1. Dezember 2020, 16:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicPowerUser`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:InitiateLayerUpload",
        "ecr-public:UploadLayerPart",
        "ecr-public:CompleteLayerUpload",
        "ecr-public:PutImage"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticContainerRegistryPublicReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf öffentliche Amazon ECR-Repositorys.

`AmazonElasticContainerRegistryPublicReadOnly`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonElasticContainerRegistryPublicReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 17:27 UTC
- Zeit bearbeitet: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticContainerRegistryPublicReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken",
        "sts:GetServiceBearerToken",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:DescribeRepositories",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeImageTags",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRegistryCatalogData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientFullAccess

Beschreibung: Bietet Root-Client-Zugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemClientFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Januar 2020, 16:27 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Client-Zugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemClientReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Januar 2020, 16:24 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemClientReadWriteAccess

Beschreibung: Bietet Lese- und Schreibclientzugriff auf ein Amazon EFS-Dateisystem

`AmazonElasticFileSystemClientReadWriteAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemClientReadWriteAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 13. Januar 2020, 16:21 UTC
- Bearbeitete Zeit: 13. Januar 2020, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemClientReadWriteAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EFS über die AWS-Managementkonsole.

`AmazonElasticFileSystemFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2015, 16:22 UTC
- Zeit bearbeitet: 7. November 2024, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:CreateAccessPoint",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "elasticfilesystem:DeleteTags",
        "elasticfilesystem:DeleteAccessPoint",
        "elasticfilesystem:DeleteFileSystemPolicy",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ModifyMountTargetSecurityGroups",
        "elasticfilesystem:PutAccountPreferences",
        "elasticfilesystem:PutBackupPolicy",
        "elasticfilesystem:PutLifecycleConfiguration",
        "elasticfilesystem:PutFileSystemPolicy",
        "elasticfilesystem:UpdateFileSystem",
        "elasticfilesystem:UpdateFileSystemProtection",
        "elasticfilesystem:TagResource",
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:Backup",
        "elasticfilesystem:Restore",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite",
        "kms:DescribeKey",
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForEFS",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticfilesystem.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForEFS",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticfilesystem.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EFS über die AWS-Managementkonsole.

`AmazonElasticFileSystemReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2015, 16:25 UTC
- Zeit bearbeitet: 7. November 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticFileSystemReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricData",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:ListTagsForResource",
        "elasticfilesystem:ReplicationRead",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemServiceRolePolicy

Beschreibung: Ermöglicht Amazon Elastic File System, AWS Ressourcen in Ihrem Namen zu verwalten

`AmazonElasticFileSystemServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. November 2019, 16:52 UTC
- Zeit bearbeitet: 7. November 2024, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticFileSystemServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:MountCapsule",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:ModifyNetworkInterfaceAttribute",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupVault",
        "backup:PutBackupVaultAccessPolicy"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-vault:aws/efs/automatic-backup-vault"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupPlan",
        "backup:CreateBackupSelection"
      ],
      "Resource" : [
        "arn:aws:backup:*:*:backup-plan:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/backup.amazonaws.com/
AWSServiceRoleForBackup"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateReplicationConfiguration",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DeleteReplicationConfiguration",
        "elasticfilesystem:ReplicationRead",
        "elasticfilesystem:ReplicationWrite"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticFileSystemsUtils

Beschreibung: Ermöglicht Kunden, AWS Systems Manager zu verwenden, um das Amazon EFS Utilities-Paket (amazon-efs-utils) auf ihren EC2 Instances automatisch zu verwalten und success/failure Benachrichtigungen CloudWatchLog zum Einhängen des EFS-Dateisystems zu erhalten.

`AmazonElasticFileSystemsUtils`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticFileSystemsUtils` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. September 2020, 15:16 Uhr UTC
- Bearbeitete Zeit: 29. September 2020, 15:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
```

```
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceEditorsRole

Beschreibung: Standardrichtlinie für die Amazon Elastic MapReduce Editors-Servicerolle.

`AmazonElasticMapReduceEditorsRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceEditorsRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2018, 21:55 Uhr UTC

- Bearbeitete Zeit: 9. Februar 2023, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceEditorsRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:elasticmapreduce:editor-id",
            "aws:elasticmapreduce:job-flow-id"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceforAutoScalingRole

Beschreibung: Amazon Elastic MapReduce für Auto Scaling. Rolle, mit der Auto Scaling Instances zu Ihrem EMR-Cluster hinzufügen und daraus entfernen kann.

`AmazonElasticMapReduceforAutoScalingRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceforAutoScalingRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 18. November 2016, 01:09 UTC
- Bearbeitete Zeit: 18. November 2016, 01:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforAutoScalingRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceforEC2Role

Beschreibung: Standardrichtlinie für die Rolle Amazon Elastic MapReduce for EC2 Service.

`AmazonElasticMapReduceforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceforEC2Role` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 11. August 2017, 23:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceforEC2Role`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "cloudwatch:*",
        "dynamodb:*",
```

```
        "ec2:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSteps",
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:MergeShards",
        "kinesis:PutRecord",
        "kinesis:SplitShard",
        "rds:Describe*",
        "s3:*",
        "sdb:*",
        "sns:*",
        "sqs:*",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:UpdatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:CreateUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:DeleteUserDefinedFunction",
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceFullAccess

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https:// docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Bietet vollen Zugriff auf Amazon Elastic MapReduce und die dafür benötigten zugrunde liegenden Dienste wie EC2 S3

`AmazonElasticMapReduceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 11. Oktober 2019, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateRoute",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
```

```
        "ec2:TerminateInstances",
        "elasticmapreduce:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:List*",
        "s3:*",
        "sdb:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReducePlacementGroupPolicy

Beschreibung: Richtlinie, die es EMR ermöglicht, EC2 Platzierungsgruppen zu erstellen, zu beschreiben und zu löschen.

`AmazonElasticMapReducePlacementGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReducePlacementGroupPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. September 2020, 00:37 UTC
- Zeit bearbeitet: 29. September 2020, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReducePlacementGroupPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Resource" : "*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups"
```

```
      ]
    },
    {
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Elastic MapReduce über die AWS-Managementkonsole.

`AmazonElasticMapReduceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 29. Juli 2020, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticMapReduceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sdb:Select",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticMapReduceRole

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https:// docs.aws.amazon.com/emr/ latest/ManagementGuide/emr - managed-iam-policies .html. Standardrichtlinie für die Amazon MapReduce Elastic-Servicerolle.

`AmazonElasticMapReduceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticMapReduceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. Juni 2020, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticMapReduceRole`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CancelSpotInstanceRequests",
```

```
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfiles",
```

```
        "iam:ListRolePolicies",
        "iam:PassRole",
        "s3:CreateBucket",
        "s3:Get*",
        "s3:List*",
        "sdb:BatchPutAttributes",
        "sdb:Select",
        "sqs:CreateQueue",
        "sqs:Delete*",
        "sqs:GetQueue*",
        "sqs:PurgeQueue",
        "sqs:ReceiveMessage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:Describe*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/spot.amazonaws.com/
AWSServiceRoleForEC2Spot*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticsearchServiceRolePolicy

Beschreibung: Erlauben Sie Amazon Elasticsearch Service, in Ihrem Namen APIs auf andere AWS Dienste wie EC2 Networking zuzugreifen.

`AmazonElasticsearchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Juli 2017, 00:15 UTC
- Bearbeitete Zeit: 23. Oktober 2023, 06:58 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonElasticsearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "Stmt1480452973134",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973135",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973136",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/ES"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_FullAccess

Beschreibung: Gewährt Benutzern vollen Zugriff auf Elastic Transcoder und den Zugriff auf zugehörige Dienste, der für die volle Funktionalität von Elastic Transcoder erforderlich ist.

`AmazonElasticTranscoder_FullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonElasticTranscoder_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. April 2018, 18:59 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "elastictranscoder.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_JobsSubmitter

Beschreibung: Erteilt Benutzern die Erlaubnis, Voreinstellungen zu ändern, Jobs einzureichen und Elastic Transcoder Transcoder-Einstellungen einzusehen. Diese Richtlinie gewährt auch einen gewissen Lesezugriff auf einige andere Dienste, die für die Nutzung der Elastic Transcode-Konsole erforderlich sind, darunter S3, IAM und SNS.

`AmazonElasticTranscoder_JobsSubmitter`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonElasticTranscoder_JobsSubmitter` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 7. Juni 2018, 21:12 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_JobsSubmitter`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "elastictranscoder:*Job",
        "elastictranscoder:*Preset",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoder_ReadOnlyAccess

Beschreibung: Gewährt Benutzern nur Lesezugriff auf Elastic Transcoder und Listenzugriff auf verwandte Dienste.

`AmazonElasticTranscoder_ReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonElasticTranscoder_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Juni 2018, 21:09 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonElasticTranscoder_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "elastictranscoder:Read*",
        "elastictranscoder:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "iam:ListRoles",
        "sns:ListTopics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonElasticTranscoderRole

Beschreibung: Standardrichtlinie für die Amazon Elastic Transcoder-Servicerolle.

`AmazonElasticTranscoderRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonElasticTranscoderRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC

- Bearbeitete Zeit: 13. Juni 2019, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonElasticTranscoderRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:Get*",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:*MultipartUpload*"
      ],
      "Sid" : "1",
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Sid" : "2",
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRCleanupPolicy

Beschreibung: Ermöglicht die Aktionen, die EMR zum Beenden und Löschen von AWS EC2 Ressourcen benötigt, wenn die EMR-Dienstrolle diese Fähigkeit verloren hat.

`AmazonEMRCleanupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. September 2017, 23:54 Uhr UTC
- Bearbeitete Zeit: 29. September 2020, 21:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRCleanupPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DeleteLaunchTemplate",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:CancelSpotInstanceRequests",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:DeleteVolume",
        "ec2:DescribePlacementGroups",
        "ec2:DeletePlacementGroup"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRContainersServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon EMR erforderlich sind

`AmazonEMRContainersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Dezember 2020, 00:38 UTC
- Zeit bearbeitet: 6. Februar 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRContainersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
```

```
        "eks:ListNodeGroups",
        "eks:DescribeNodeGroup",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ImportCertificate",
        "acm:AddTagsToCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/emr-container:endpoint:managed-certificate" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRFullAccessPolicy_v2

Beschreibung: Bietet vollen Zugriff auf Amazon EMR

`AmazonEMRFullAccessPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEMRFullAccessPolicy_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2021, 01:50 UTC
- Bearbeitete Zeit: 27. März 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRFullAccessPolicy_v2`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "RunJobFlowExplicitlyWithEMRManagedTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:RunJobFlow"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddInstanceFleet",
        "elasticmapreduce:AddInstanceGroups",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:CreateEditor",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteEditor",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
```

```
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ModifyCluster",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:ModifyInstanceGroups",
        "elasticmapreduce:OpenEditorInConsole",
        "elasticmapreduce:PutAutoScalingPolicy",
        "elasticmapreduce:PutBlockPublicAccessConfiguration",
        "elasticmapreduce:PutManagedScalingPolicy",
        "elasticmapreduce:RemoveAutoScalingPolicy",
        "elasticmapreduce:RemoveManagedScalingPolicy",
        "elasticmapreduce:RemoveTags",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:StartEditor",
        "elasticmapreduce:StopEditor",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleForElasticMapReduce",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_DefaultRole_V2",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "elasticmapreduce.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "ElasticMapReduceServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
elasticmapreduce.amazonaws.com*/AWSServiceRoleForEMRCleanup*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "elasticmapreduce.amazonaws.com",
            "elasticmapreduce.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleUIActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "s3:ListAllMyBuckets",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRReadOnlyAccessPolicy_v2

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EMR und die zugehörigen CloudWatch Metriken.

`AmazonEMRReadOnlyAccessPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEMRReadOnlyAccessPolicy_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2021, 01:39 UTC
- Bearbeitete Zeit: 2. August 2023, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEMRReadOnlyAccessPolicy_v2`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticMapReduceActions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeEditor",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeReleaseLabel",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListEditors",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ViewEventsFromAllClustersInConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewMetricsInEMRConsole",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRServerlessServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für den Betrieb von Amazon erforderlich sind EMRServerless

`AmazonEMRServerlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Mai 2022, 23:15 UTC
- Bearbeitete Zeit: 25. Januar 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEMRServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2PolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/EMRServerless",
            "AWS/Usage"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEMRServicePolicy_v2

Beschreibung: Diese Richtlinie wird für die Amazon EMR-Servicerolle verwendet und sollte NICHT für andere IAM-Benutzer oder -Rollen in Ihrem Konto verwendet werden. Die Richtlinie gewährt Berechtigungen zum Erstellen und Verwalten von Ressourcen im Zusammenhang mit EMR und verwandten Diensten, die für den Betrieb Ihres EMR-Clusters erforderlich sind.

`AmazonEMRServicePolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEMRServicePolicy_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. März 2021, 01:11 Uhr UTC
- Bearbeitete Zeit: 03. März 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateInTaggedNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateWithEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFleet",
        "ec2:RunInstances",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateEMRTaggedLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEMRTaggedInstancesAndVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ResourcesToLaunchEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/ami-*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
```

```
        "arn:aws:ec2:*:*:placement-group/EMR_*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:dedicated-host/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "ManageEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "ManageTagsOnEMRTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceNeededForPrivateSubnet",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateTaggedEMRResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateFleet",
            "CreateLaunchTemplate",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "TagPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:placement-group/EMR_*"
      ]
    },
    {
      "Sid" : "ListActionsForEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "CreateDefaultSecurityGroupInVPCWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
    {
      "Sid" : "TagOnCreateDefaultSecurityGroupWithEMRTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "ManageSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateEMRPlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreatePlacementGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:placement-group/EMR_*"
    },
    {
      "Sid" : "DeletePlacementGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeletePlacementGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsForCapacityReservations",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
```

```
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*_EMR_Auto_Scaling"
    },
    {
      "Sid" : "PassRoleForAutoScaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_AutoScaling_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "application-autoscaling.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "PassRoleForEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "CreateAndModifyEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "CreateEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    },
    {
      "Sid" : "TagEmrServiceVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies" : "true",
          "aws:RequestTag/Name" : "emr-service-vpce"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESCognitoAccess

Beschreibung: Bietet eingeschränkten Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice.

`AmazonESCognitoAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonESCognitoAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2018, 22:29 UTC
- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESCognitoAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
```

```
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:SetIdentityPoolRoles",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon ES-Konfigurationsservice.

`AmazonESFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonESFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Oktober 2015, 19:14 UTC
- Zeit bearbeitet: 1. Oktober 2015, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "es:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonESReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon ES-Konfigurationsservice.

`AmazonESReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonESReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Oktober 2015, 19:18 UTC
- Bearbeitete Zeit: 3. Oktober 2018, 03:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonESReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeApiDestinationsServiceRolePolicy

Beschreibung: Ermöglicht EventBridge den Zugriff auf Secret Manager-Ressourcen in Ihrem Namen.

`AmazonEventBridgeApiDestinationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Februar 2021, 20:52 UTC
- Bearbeitete Zeit: 29. Mai 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeApiDestinationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : [
```

```
            "arn:aws:secretsmanager:*:*:secret:events!connection/*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/EventBridgeApiDestinations" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge.

`AmazonEventBridgeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Juli 2019, 14:08 UTC
- Bearbeitete Zeit: 22. Januar 2025, 01:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleAccessForEventBridge",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgePipesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:03 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgePipesActions",
      "Effect" : "Allow",
      "Action" : "pipes:*",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesOperatorAccess

Beschreibung: Bietet schreibgeschützten Zugriff und Bedienerzugriff (Fähigkeit, Pipes zu beenden und zu starten) auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgePipesOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesOperatorAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource",
```

```
        "pipes:StartPipe",
        "pipes:StopPipe"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgePipesReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EventBridge Pipes.

`AmazonEventBridgePipesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgePipesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2022, 17:04 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgePipesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon EventBridge.

`AmazonEventBridgeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Juli 2019, 13:59 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
```

```
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchedulerFullAccess

Beschreibung: Die AmazonEventBridgeSchedulerFullAccess verwaltete Richtlinie gewährt Berechtigungen zur Verwendung aller EventBridge Scheduler-Aktionen für Zeitpläne und Zeitplangruppen.

`AmazonEventBridgeSchedulerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeSchedulerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 18:37 UTC
- Bearbeitete Zeit: 16. Mai 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchedulerReadOnlyAccess

Beschreibung: Die AmazonEventBridgeSchedulerReadOnlyAccess verwaltete Richtlinie gewährt nur Leseberechtigungen zum Anzeigen von Details zu Ihren Zeitplänen und Zeitplangruppen

`AmazonEventBridgeSchedulerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeSchedulerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 10. November 2022, 18:50 UTC
- Bearbeitete Zeit: 16. Mai 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchedulerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeSchemasFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2019, 23:12 Uhr UTC
- Zeit bearbeitet: 28. November 2019, 23:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonEventBridgeManageRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*Schemas*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon EventBridge Schemas.

`AmazonEventBridgeSchemasReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonEventBridgeSchemasReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2019, 23:05 UTC
- Bearbeitete Zeit: 1. Mai 2020, 00:50 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonEventBridgeSchemasReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonEventBridgeSchemasReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "schemas:ListDiscoverers",
        "schemas:DescribeDiscoverer",
        "schemas:ListRegistries",
        "schemas:DescribeRegistry",
        "schemas:SearchSchemas",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:DescribeSchema",
```

```
        "schemas:GetDiscoveredSchema",
        "schemas:DescribeCodeBinding",
        "schemas:GetCodeBindingSource",
        "schemas:ListTagsForResource",
        "schemas:GetResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEventBridgeSchemasServiceRolePolicy

Beschreibung: Erteilt Berechtigungen für verwaltete Regeln, die von EventBridge Amazon-Schemas erstellt wurden.

`AmazonEventBridgeSchemasServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2019, 01:10 Uhr UTC
- Bearbeitete Zeit: 27. November 2019, 01:10 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEventBridgeSchemasServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:EnableRule",
        "events:DisableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*Schemas-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonEVSServiceRolePolicy

Beschreibung: Erteilt EVS die Erlaubnis, Ressourcen in Ihrem Namen zu verwalten

`AmazonEVSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Mai 2025, 23:37 UTC
- Bearbeitete Zeit: 14. August 2025, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonEVSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ManageSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateEniWithTagStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "TagOnCreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonEVSManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageInstanceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DescribeInstanceAndVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageVolumeStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonEVSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "UpdateSecurityGroupStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "CloudWatchPutMetricDataStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/EVS"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFISServiceRolePolicy

Beschreibung: Richtlinie, die es der AWS FIS ermöglicht, die Überwachung und die Auswahl der Ressourcen für Experimente zu verwalten.

`AmazonFISServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2020, 21:18 Uhr UTC
- Bearbeitete Zeit: 25. Oktober 2022, 09:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFISServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "fis.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "EventBridgeDescribe",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Tagging",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeUserResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "iam:GetUser",
        "iam:GetRole",
        "iam:ListUsers",
        "iam:ListRoles",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "ecs:DescribeClusters",
        "ecs:DescribeTasks",
        "ecs:ListTasks",
        "eks:DescribeNodegroup",
```

```
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonForecastFullAccess

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Forecast

`AmazonForecastFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonForecastFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 01:52 UTC
- Bearbeitete Zeit: 18. Januar 2019, 01:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonForecastFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "forecast:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFraudDetectorFullAccessPolicy

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Fraud Detector

`AmazonFraudDetectorFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFraudDetectorFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 22:46 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFraudDetectorFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "frauddetector:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListEndpoints",
        "sagemaker:DescribeEndpoint"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "frauddetector.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFreeRTOSFullAccess

Beschreibung: Vollständige Zugriffsrichtlinie für Amazon FreeRTOS

`AmazonFreeRTOSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFreeRTOSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 15:32 UTC
- Zeit bearbeitet: 29. November 2017, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFreeRTOSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "freertos:*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFreeRTOSOTAUpdate

Beschreibung: Ermöglicht dem Benutzer den Zugriff auf Amazon FreeRTOS OTA Update

`AmazonFreeRTOSOTAUpdate`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFreeRTOSOTAUpdate` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. August 2018, 22:43 UTC
- Bearbeitete Zeit: 18. Dezember 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonFreeRTOSOTAUpdate`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::afr-ota*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "signer:StartSigningJob",
        "signer:DescribeSigningJob",
        "signer:GetSigningProfile",
        "signer:PutSigningProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteJob",
        "iot:DescribeJob"
      ],
      "Resource" : "arn:aws:iot:*:*:job/AFR_OTA*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream"
      ],
      "Resource" : "arn:aws:iot:*:*:stream/AFR_OTA*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateStream",
        "iot:CreateJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste über die AWS-Managementkonsole.

`AmazonFSxConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFSxConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. November 2018, 16:36 UTC
- Zeit bearbeitet: 5. November 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListResourcesAssociatedWithFSxFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "kms:ListAliases",
        "logs:DescribeLogGroups",
        "s3:ListBucket",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
```

```
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateFSxSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxConsoleReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste über die AWS-Managementkonsole.

`AmazonFSxConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFSxConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:35 UTC
- Bearbeitete Zeit: 25. Februar 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FSxReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "ds:DescribeDirectories",
        "ec2:DescribeNetworkInterfaceAttribute",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "firehose:ListDeliveryStreams",
        "fsx:Describe*",
        "fsx:ListTagsForResource",
        "kms:DescribeKey",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Dienste.

`AmazonFSxFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFSxFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:34 UTC
- Bearbeitete Zeit: 25. Juni 2025, 17:52 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonFSxFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ViewAWSDSDirectories",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FullAccessToFSx",
      "Effect" : "Allow",
      "Action" : [
        "fsx:AssociateFileGateway",
        "fsx:AssociateFileSystemAliases",
        "fsx:CancelDataRepositoryTask",
        "fsx:CopyBackup",
        "fsx:CopySnapshotAndUpdateVolume",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:CreateBackup",
        "fsx:CreateDataRepositoryAssociation",
        "fsx:CreateDataRepositoryTask",
        "fsx:CreateFileCache",
        "fsx:CreateFileSystem",
        "fsx:CreateFileSystemFromBackup",
        "fsx:CreateSnapshot",
        "fsx:CreateStorageVirtualMachine",
```

```
        "fsx:CreateVolume",
        "fsx:CreateVolumeFromBackup",
        "fsx:DetachAndDeleteS3AccessPoint",
        "fsx:DeleteBackup",
        "fsx:DeleteDataRepositoryAssociation",
        "fsx:DeleteFileCache",
        "fsx:DeleteFileSystem",
        "fsx:DeleteSnapshot",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume",
        "fsx:DescribeAssociatedFileGateways",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeDataRepositoryTasks",
        "fsx:DescribeFileCaches",
        "fsx:DescribeFileSystemAliases",
        "fsx:DescribeFileSystems",
        "fsx:DescribeS3AccessPointAttachments",
        "fsx:DescribeSharedVpcConfiguration",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:DisassociateFileGateway",
        "fsx:DisassociateFileSystemAliases",
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:ReleaseFileSystemNfsV3Locks",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:UpdateDataRepositoryAssociation",
        "fsx:UpdateFileCache",
        "fsx:UpdateFileSystem",
        "fsx:UpdateSharedVpcConfiguration",
        "fsx:UpdateSnapshot",
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLRForFSx",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSLRForLustreS3Integration",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "s3.data-source.lustre.fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateLogsForFSxWindowsAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/fsx/*"
      ]
    },
    {
      "Sid" : "WriteToAmazonKinesisDataFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
      ]
    },
```

```
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonFSx" : "ManagedByAmazonFSx"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeEC2VpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "fsx.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageCrossAccountDataReplication",
      "Effect" : "Allow",
      "Action" : [
        "fsx:PutResourcePolicy",
```

```
        "fsx:GetResourcePolicy",
        "fsx:DeleteResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon FSx.

`AmazonFSxReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonFSxReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 16:33 UTC
- Zeit bearbeitet: 28. November 2018, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonFSxReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:Describe*",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonFSxServiceRolePolicy

Beschreibung: Ermöglicht Amazon FSx , AWS Ressourcen in Ihrem Namen zu verwalten

`AmazonFSxServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. November 2018, 10:38 UTC
- Bearbeitete Zeit: 22. Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonFSxServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateFileSystem",
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/FSx"
        }
      }
    },
    {
      "Sid" : "TagResourceNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonFSx.FileSystemId"
        }
      }
    },
    {
```

```
      "Sid" : "ManageNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonFSx.FileSystemId" : "false"
        }
      }
    },
    {
      "Sid" : "ManageRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2:DeleteRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/fsx/*"
```

```
    },
    {
      "Sid" : "ManageAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGlacierFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Glacier über die AWS-Managementkonsole.

`AmazonGlacierFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonGlacierFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "glacier:*",
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGlacierReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Glacier über die AWS-Managementkonsole.

`AmazonGlacierReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonGlacierReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 5. Mai 2016, 18:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGlacierReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glacier:DescribeJob",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetJobOutput",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:GetVaultNotifications",
        "glacier:ListJobs",
        "glacier:ListMultipartUploads",
        "glacier:ListParts",
        "glacier:ListTagsForVault",
        "glacier:ListVaults"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaAthenaAccess

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Athena und die Abhängigkeiten, die erforderlich sind, um das Abfragen und Schreiben von Ergebnissen aus dem Amazon Athena-Plugin in Amazon Grafana in S3 zu ermöglichen.

`AmazonGrafanaAthenaAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonGrafanaAthenaAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. November 2021, 17:11 Uhr UTC
- Bearbeitete Zeit: 22. November 2021, 17:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaAthenaAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetWorkGroup",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::grafana-athena-query-results-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaCloudWatchAccess

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon CloudWatch und die Abhängigkeiten, die für die Verwendung CloudWatch als Datenquelle in Amazon Managed Grafana erforderlich sind.

`AmazonGrafanaCloudWatchAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonGrafanaCloudWatchAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. März 2023, 22:41 UTC
- Bearbeitete Zeit: 24. März 2023, 22:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaCloudWatchAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
```

```
        "cloudwatch:GetMetricData",
        "cloudwatch:GetInsightRuleReport"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:GetLogGroupFields",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:GetLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks",
        "oam:ListAttachedLinks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaRedshiftAccess

Beschreibung: Diese Richtlinie gewährt begrenzten Zugriff auf Amazon Redshift und die Abhängigkeiten, die für die Verwendung des Amazon Redshift Redshift-Plug-ins in Amazon Grafana erforderlich sind.

`AmazonGrafanaRedshiftAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonGrafanaRedshiftAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. November 2021, 23:15 Uhr UTC
- Bearbeitete Zeit: 26. November 2021, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonGrafanaRedshiftAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:ListTables",
        "redshift-data:ListSchemas"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GrafanaDataSource" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGrafanaServiceLinkedRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon Grafana verwaltet oder verwendet werden.

`AmazonGrafanaServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. November 2022, 23:10 UTC
- Zeit bearbeitet: 8. November 2022, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGrafanaServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonGrafanaManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AmazonGrafanaManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AmazonGrafanaManaged" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyFullAccess

Beschreibung: Bietet vollen Zugriff auf die Nutzung von Amazon GuardDuty.

`AmazonGuardDutyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonGuardDutyFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. November 2017, 22:31 UTC
- Zeit bearbeitet: 20. November 2025, 02:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonGuardDutyFullAccessSid1",
      "Effect" : "Allow",
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ActionsForOrganizationsSid1",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamGetRoleSid1",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyFullAccess_v2

Beschreibung: Bietet vollen Zugriff auf Amazon GuardDuty

`AmazonGuardDutyFullAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonGuardDutyFullAccess_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2025, 20:22 UTC
- Zeit bearbeitet: 20. November 2025, 02:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyFullAccess_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : "guardduty:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateGuardDutyServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyOrganizationsAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "guardduty.amazonaws.com",
```

```
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyIamRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    },
    {
      "Sid" : "AllowPassRoleToMalwareProtection",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "malware-protection-plan.guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyMalwareProtectionServiceRolePolicy

Beschreibung: Der GuardDuty Malware-Schutz verwendet die angegebene Service-Linked Role (SLR). AWSService RoleForAmazonGuardDutyMalwareProtection Diese dienstbezogene Rolle ermöglicht es dem GuardDuty Malware-Schutz, Scans ohne Agenten durchzuführen, um Malware zu erkennen. Sie GuardDuty ermöglicht das Erstellen von Snapshots in Ihrem Konto und das Teilen der Snapshots mit dem GuardDuty Dienstkonto, um nach Malware zu suchen. Es wertet diese gemeinsam genutzten Snapshots aus und bezieht die abgerufenen EC2 Instanz-Metadaten in die Ergebnisse des GuardDuty Malware-Schutzes ein. Die mit dem AWSService RoleForAmazonGuardDutyMalwareProtection Dienst verknüpfte Rolle vertraut darauf, dass der Service malware protection.guardduty.amazonaws.com die Rolle übernimmt.

`AmazonGuardDutyMalwareProtectionServiceRolePolicy`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juli 2022, 19:06 UTC
- Bearbeitete Zeit: 25. Januar 2024, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyMalwareProtectionServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTasks",
        "ecs:DescribeTasks",
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSnapshotVolumeConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotConditionalStatement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyScanId"
        }
      }
    },
    {
```

```
      "Sid" : "CreateTagsPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    },
    {
      "Sid" : "AddTagsToSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyExcluded",
            "GuardDutyFindingDetected"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteAndShareSnapshotPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "PreventPublicAccessToSnapshotPermission",
      "Effect" : "Deny",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/group" : "all"
        }
      }
    },
    {
      "Sid" : "CreateGrantPermission",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermission",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "GuardDutyLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
      "Sid" : "GuardDutyLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
    },
    {
      "Sid" : "EBSDirectAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ebs:GetSnapshotBlock",
        "ebs:ListSnapshotBlocks"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/GuardDutyScanId" : "*"
        },
        "Null" : {
          "aws:ResourceTag/GuardDutyExcluded" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf GuardDuty Amazon-Ressourcen

`AmazonGuardDutyReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonGuardDutyReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 22:29 Uhr UTC
- Bearbeitete Zeit: 16. November 2023, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonGuardDutyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonGuardDutyServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die von Amazon Guard Duty verwendet oder verwaltet werden

`AmazonGuardDutyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. November 2017, 20:12 Uhr UTC
- Bearbeitete Zeit: 12. August 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonGuardDutyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyGetDescribeListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeTransitGatewayAttachments",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ecs:ListClusters",
        "ecs:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GuardDutyCreateSLRPolicy",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        },
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.guardduty-data",
            "com.amazonaws.*.guardduty-data-fips"
          ]
        }
      }
    },
    {
      "Sid" : "GuardDutyModifyDeleteVpcEndpointPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutySecurityGroupManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/GuardDutyManaged" : false
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/GuardDutyManaged" : "*"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateSecurityGroupForVpcPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyCreateEksAddonPolicy",
      "Effect" : "Allow",
      "Action" : "eks:CreateAddon",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEksAddonManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
```

```
    },
    {
      "Sid" : "GuardDutyEksClusterTagResourcePolicy",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "GuardDutyManaged"
        }
      }
    },
    {
      "Sid" : "GuardDutyEcsPutAccountSettingsDefaultPolicy",
      "Effect" : "Allow",
      "Action" : "ecs:PutAccountSettingDefault",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:account-setting" : [
            "guardDutyActivate"
          ]
        }
      }
    },
    {
      "Sid" : "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:DeleteAssociation",
        "ssm:UpdateAssociation",
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmAddTagsToResourcePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:association/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "GuardDutyManaged"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/GuardDutyManaged" : "true"
        }
      }
    },
    {
      "Sid" : "SsmCreateUpdateAssociationInstanceDocumentPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
    },
    {
      "Sid" : "SsmSendCommandPermission",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin"
      ]
    },
    {
      "Sid" : "SsmGetCommandStatus",
      "Effect" : "Allow",
      "Action" : "ssm:GetCommandInvocation",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHealthLakeFullAccess

Beschreibung: Bietet vollen Zugriff auf den HealthLake Amazon-Service.

`AmazonHealthLakeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHealthLakeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 01:07 UTC
- Bearbeitete Zeit: 17. Februar 2021, 01:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "healthlake:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "healthlake.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHealthLakeReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf den HealthLake Amazon-Service.

`AmazonHealthLakeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHealthLakeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 02:43 UTC
- Bearbeitete Zeit: 17. Februar 2021, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHealthLakeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "healthlake:ListFHIRDatastores",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:GetCapabilities",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:List*",
        "honeycode:Get*",
        "honeycode:Describe*",
        "honeycode:Query*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeServiceRolePolicy

Beschreibung: Für Amazon Honeycode ist eine servicebezogene Rolle erforderlich, um auf Ihre Ressourcen zugreifen zu können.

`AmazonHoneycodeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2020, 18:03 UTC
- Zeit bearbeitet: 18. November 2020, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonHoneycodeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeTeamAssociationFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode Team Association über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeTeamAssociationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeTeamAssociationFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations",
        "honeycode:ApproveTeamAssociation",
        "honeycode:RejectTeamAssociation"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeTeamAssociationReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode Team Association über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeTeamAssociationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeTeamAssociationReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:27 UTC
- Bearbeitete Zeit: 24. Juni 2020, 20:27 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeTeamAssociationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:ListTeamAssociations"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeWorkbookFullAccess

Beschreibung: Bietet vollen Zugriff auf Honeycode Workbook über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeWorkbookFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeWorkbookFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:InvokeScreenAutomation",
        "honeycode:BatchCreateTableRows",
        "honeycode:BatchDeleteTableRows",
        "honeycode:BatchUpdateTableRows",
        "honeycode:BatchUpsertTableRows",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
```

```
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows",
        "honeycode:StartTableDataImportJob"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonHoneycodeWorkbookReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Honeycode Workbook über das AWS-Managementkonsole und das SDK.

`AmazonHoneycodeWorkbookReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonHoneycodeWorkbookReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 20:28 UTC
- Bearbeitete Zeit: 1. Dezember 2020, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonHoneycodeWorkbookReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "honeycode:GetScreenData",
        "honeycode:DescribeTableDataImportJob",
        "honeycode:ListTableColumns",
        "honeycode:ListTableRows",
        "honeycode:ListTables",
        "honeycode:QueryTableRows"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2AgentlessServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf Sicherheitsbewertungen, die für die Durchführung ohne Agenten AWS-Services erforderlich sind

`AmazonInspector2AgentlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. November 2023, 15:18 Uhr UTC
- Bearbeitete Zeit: 20. November 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2AgentlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "InstanceIdentification",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetSnapshotData",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAnyInstanceOrVolume",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "DenyCreateSnapshotsOnExcludedInstances",
      "Effect" : "Deny",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsOnAnySnapshotOnlyWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
```

```
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "CreateSnapshots"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "InspectorScan"
        }
      }
    },
    {
      "Sid" : "DeleteOnlySnapshotsTaggedForScanning",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/InspectorScan" : "*"
        }
      }
    },
    {
      "Sid" : "DenyKmsDecryptForExcludedKeys",
      "Effect" : "Deny",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceTag/InspectorEc2Exclusion" : "true"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksVolContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "vol-*"
        }
      }
    },
    {
      "Sid" : "DecryptSnapshotBlocksSnapContext",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "snap-*"
        }
      }
    },
    {
      "Sid" : "DescribeKeysForEbsOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListKeyResourceTags",
      "Effect" : "Allow",
      "Action" : "kms:ListResourceTags",
      "Resource" : "arn:aws:kms:*:*:key/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2FullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Inspector und Zugriff auf andere verwandte Dienste wie Organisationen.

`AmazonInspector2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspector2FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 19:10 Uhr UTC
- Bearbeitete Zeit: 25. April 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2FullAccess_v2

Beschreibung: Bietet vollen Zugriff auf Amazon Inspector und Zugriff auf andere verwandte Dienste wie Organisationen mit eingeschränktem organisatorischem Zugriff.

`AmazonInspector2FullAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspector2FullAccess_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 03. Juli 2025, 16:07 UTC
- Bearbeitete Zeit: 14. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2FullAccess_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ManagedCisPolicy

Beschreibung: Dies ist eine verwaltete Richtlinie, die Kunden ihren Rollen zuordnen sollten, um mit dem Inspektor-Service für CIS-Scans zu kommunizieren

`AmazonInspector2ManagedCisPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspector2ManagedCisPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Januar 2024, 16:31 UTC
- Bearbeitete Zeit: 24. Januar 2024, 16:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ManagedCisPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "PermissionsForCISScans",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:StartCisSession",
        "inspector2:StopCisSession",
        "inspector2:SendCisSessionTelemetry",
        "inspector2:SendCisSessionHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf den Amazon Inspector2-Service und die entsprechenden Support-Services

`AmazonInspector2ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspector2ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2022, 14:45 UTC
- Bearbeitete Zeit: 14. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspector2ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "inspector2:BatchGet*",
        "inspector2:List*",
        "inspector2:Describe*",
        "inspector2:Get*",
        "inspector2:Search*",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListPoliciesForInspectorPolicyType",
      "Effect" : "Allow",
      "Action" : "organizations:ListPolicies",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AllowDescribeResourcePolicyForDelegation",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeResourcePolicy",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDescribeEffectivePolicyForInspector",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeEffectivePolicy",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:PolicyType" : [
            "INSPECTOR_POLICY"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspector2ServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf die für die Durchführung von Sicherheitsbewertungen AWS-Services erforderlichen Daten

`AmazonInspector2ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2021, 20:27 UTC
- Zeit bearbeitet: 10. November 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspector2ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TirosPolicy",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAddresses",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
```

```
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:ListImages",
        "ecr:PutRegistryScanningConfiguration",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "ssm:DescribeAssociation",
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:ListAssociations",
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPackageVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunction",
        "lambda:GetLayerVersion",
        "lambda:ListTags",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GatherInventory",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:StartAssociationsOnce",
        "ssm:UpdateAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AmazonInspector2-*",
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "GatherInventoryDeleteAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "DataSyncCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
      ]
    },
    {
      "Sid" : "ManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
```

```
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
      ]
    },
    {
      "Sid" : "LambdaCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetAccountConfiguration",
        "codeguru-security:GetFindings",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:BatchGetFindings",
        "codeguru-security:DeleteScansByCategory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CodeGuruCodeVulnerabilityScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedRolePolicies",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "codeguru-security.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "Ec2DeepInspection",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:GetParameters",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-
paths"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListServiceLinkedChannels",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToRunInvokeCisSpecificDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
      ]
    },
    {
      "Sid" : "AllowToRunCisCommandsToSpecificResources",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToPutCloudwatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Inspector2"
        }
      }
    },
    {
      "Sid" : "AllowListAccessToECSAndEKS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAccessToECSTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowInspectorEnablementForAwsOrgPolicy",
      "Effect" : "Allow",
      "Action" : [
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
```

```
        "inspector2:AssociateMember"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowInspectorServiceDelegatedAdminFromAwsOrg",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Inspector.

`AmazonInspectorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspectorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 21. Dezember 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "inspector.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/
AWSServiceRoleForAmazonInspector",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "inspector.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorReadOnlyAccess

Beschreibung: Bietet nur Lesezugriff auf Amazon Inspector.

`AmazonInspectorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonInspectorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 17:08 UTC
- Bearbeitete Zeit: 1. Oktober 2019, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonInspectorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "sns:ListTopics",
        "events:DescribeRule",
        "events:ListRuleNamesByTarget"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonInspectorServiceRolePolicy

Beschreibung: Gewährt Amazon Inspector Zugriff auf die für die Durchführung von Sicherheitsbewertungen AWS-Services erforderlichen Daten

`AmazonInspectorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. November 2017, 15:48 Uhr UTC
- Bearbeitete Zeit: 11. September 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonInspectorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "directconnect:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeTags",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
```

```
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKendraFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kendra über die AWS-Managementkonsole.

`AmazonKendraFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKendraFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:15 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kendra.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "kms:ListKeys",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonKendra-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kendra:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKendraReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Kendra über die AWS-Managementkonsole.

`AmazonKendraReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKendraReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:13 UTC
- Bearbeitete Zeit: 27. Mai 2021, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKendraReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kendra:Describe*",
        "kendra:List*",
        "kendra:Query",
        "kendra:GetQuerySuggestions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Keyspaces

`AmazonKeyspacesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKeyspacesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 23. April 2020, 17:06 UTC
- Bearbeitete Zeit: 30. Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CassandraFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "kms:DescribeKey",
```

```
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudwatchAlarmsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApplicationAutoscalingServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesReplicationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
replication.cassandra.amazonaws.com/AWSServiceRoleForKeyspacesReplication",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "replication.cassandra.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "KeyspacesCDCServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra-
streams.amazonaws.com/AWSServiceRoleForAmazonKeyspacesCDC",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra-streams.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2VpcReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Keyspaces

`AmazonKeyspacesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKeyspacesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. April 2020, 17:07 UTC
- Bearbeitete Zeit: 30. Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKeyspacesReadOnlyAccess_v2

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Keyspaces und verwandte AWS Dienste.

`AmazonKeyspacesReadOnlyAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKeyspacesReadOnlyAccess_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. September 2023, 17:01 UTC
- Bearbeitete Zeit: 27. Juni 2025, 22:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKeyspacesReadOnlyAccess_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:ListStreams",
        "cassandra:GetStream",
        "cassandra:GetShardIterator",
        "cassandra:GetRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kinesis Analytics über die AWS-Managementkonsole.

`AmazonKinesisAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. September 2016, 19:01 UTC
- Bearbeitete Zeit: 21. September 2016, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisanalytics:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:DeleteStream",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/kinesis-analytics*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisAnalyticsReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Kinesis Analytics über die. AWS-Managementkonsole

`AmazonKinesisAnalyticsReadOnly`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisAnalyticsReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. September 2016, 18:16 Uhr UTC
- Bearbeitete Zeit: 21. September 2016, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisAnalyticsReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicyVersions",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFirehoseFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisFirehoseFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 18:45 Uhr UTC
- Zeit bearbeitet: 7. Oktober 2015, 18:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFirehoseReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Kinesis Firehose Delivery Streams.

`AmazonKinesisFirehoseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisFirehoseReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2015, 18:43 UTC
- Zeit bearbeitet: 7. Oktober 2015, 18:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFirehoseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "firehose:Describe*",
        "firehose:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Streams über die AWS-Managementkonsole.

`AmazonKinesisFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC

- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesis:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Streams über die AWS-Managementkonsole.

`AmazonKinesisReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:Get*",
        "kinesis:List*",
        "kinesis:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisVideoStreamsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Kinesis Video Streams über die AWS-Managementkonsole.

`AmazonKinesisVideoStreamsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisVideoStreamsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2017, 23:27 UTC
- Zeit bearbeitet: 1. Dezember 2017, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "kinesisvideo:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonKinesisVideoStreamsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Kinesis Video Streams über die AWS-Managementkonsole.

`AmazonKinesisVideoStreamsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonKinesisVideoStreamsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2017, 23:14 Uhr UTC

- Zeit bearbeitet: 1. Dezember 2017, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonKinesisVideoStreamsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLaunchWizard_Fullaccess

Beschreibung: Voller Zugriff auf den AWS Startassistenten und andere erforderliche Dienste.

`AmazonLaunchWizard_Fullaccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLaunchWizard_Fullaccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. August 2020, 17:47 UTC
- Bearbeitete Zeit: 22. Februar 2023, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizard_Fullaccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:List*",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
```

```
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
```

```
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLog*",
        "logs:PutLogEvents",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
```

```
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*",
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogStream",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
```

```
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "logs:CreateLogGroup",
        "logs:GetLogDelivery",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
        "ssm:GetCommandInvocation",
```

```
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLog*",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*:*:*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
```

```
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
        "aws:RequestTag/Name" : [
          "LaunchWizard*"
        ]
      }
    }
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "fsx:DescribeFileSystems"
    ],
    "Resource" : "*"
  },
  {
    "Effect" : "Allow",
    "Action" : [
      "servicecatalog:CreatePortfolio",
      "servicecatalog:DescribePortfolio",
      "servicecatalog:CreateConstraint",
      "servicecatalog:CreateProduct",
      "servicecatalog:AssociatePrincipalWithPortfolio",
      "servicecatalog:CreateProvisioningArtifact",
      "servicecatalog:TagResource",
      "servicecatalog:UntagResource"
    ],
    "Resource" : [
      "arn:aws:servicecatalog:*:*:*/*",
      "arn:aws:catalog:*:*:*/*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "aws:CalledVia" : "launchwizard.amazonaws.com"
      }
    }
  },
  {
    "Sid" : "VisualEditor0",
    "Effect" : "Allow",
    "Action" : [
      "ssm:CreateAssociation",
      "ssm:DeleteAssociation"
    ],
    "Resource" : "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
    "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:LaunchWizard*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLaunchWizardFullAccessV2

Beschreibung: Voller Zugriff auf den AWS Startassistenten und andere erforderliche Dienste.

`AmazonLaunchWizardFullAccessV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLaunchWizardFullAccessV2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. September 2023, 17:14 Uhr UTC
- Bearbeitete Zeit: 1. September 2023, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLaunchWizardFullAccessV2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppInsightsActions0",
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupActions0",
      "Effect" : "Allow",
```

```
      "Action" : "resource-groups:List*",
      "Resource" : "*"
    },
    {
      "Sid" : "Route53Actions0",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets",
        "route53:GetChange",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions0",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsActions0",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:List*",
        "cloudwatch:Get*",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Ec2Actions0",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateVpc",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Actions1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AllocateHosts",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateVolume",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVolumeAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVolume",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteKeyPair",
        "ec2:DeleteNatGateway",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DeleteSnapshot",
        "ec2:AssociateRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DetachNetworkInterface",
        "ec2:DisassociateAddress",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:GetLaunchTemplateData",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:GetConsoleOutput",
        "ec2:GetPasswordData",
        "ec2:ReleaseAddress",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:ModifyInstancePlacement",
        "ec2:DeletePlacementGroup",
        "ec2:CreatePlacementGroup",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget",
        "ds:AddIpRoutes",
        "ds:CreateComputer",
        "ds:CreateMicrosoftAD",
        "ds:DeleteDirectory",
        "servicecatalog:AssociateProductWithPortfolio",
        "cloudformation:GetTemplateSummary",
        "sts:GetCallerIdentity"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:Get*",
        "cloudformation:ListStacks",
        "cloudformation:SignalResource",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/LaunchWizard*/*",
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights*/*"
      ]
    },
    {
      "Sid" : "Ec2Actions2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
      "Sid" : "IamActions0",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
```

```
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
    },
    {
      "Sid" : "IamActions1",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonEC2RoleForLaunchWizard",
        "arn:aws:iam::*:role/service-role/AmazonLambdaRoleForLaunchWizard",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AutoScalingActions0",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "sns:ListSubscriptionsByTopic",
        "sns:Publish",
        "ssm:DeleteDocument",
```

```
        "ssm:DeleteParameter*",
        "ssm:DescribeDocument*",
        "ssm:GetDocument",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/LaunchWizard*",
        "arn:aws:sns:*:*:*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
LaunchWizard*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/
LaunchWizard*",
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions0",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunShellScript"
      ]
    },
    {
      "Sid" : "SsmActions1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        }
      }
    },
    {
```

```
      "Sid" : "SsmActions2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:DescribeDocument",
        "ssm:GetDocument",
        "ssm:ListTagsForResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/LaunchWizard*",
        "arn:aws:ssm:*:*:document/LaunchWizard*"
      ]
    },
    {
      "Sid" : "SsmActions3",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:DescribeAccountLimits",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "ds:Describe*",
        "ds:ListAuthorizedApplications",
        "ec2:Describe*",
        "ec2:Get*",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:List*",
        "resource-groups:Get*",
        "resource-groups:List*",
        "servicequotas:GetServiceQuota",
        "servicequotas:ListServiceQuotas",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "ssm:CreateDocument",
        "ssm:DescribeAutomation*",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters",
        "ssm:GetAutomationExecution",
```

```
        "ssm:GetCommandInvocation",
        "ssm:GetParameter*",
        "ssm:GetConnectionStatus",
        "ssm:ListCommand*",
        "ssm:ListDocument*",
        "ssm:ListInstanceAssociations",
        "ssm:SendAutomationSignal",
        "tag:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-definition/LaunchWizard-*:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormationActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:List*",
        "cloudformation:Describe*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/LaunchWizard*/"
    },
    {
      "Sid" : "IamActions2",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "autoscaling.amazonaws.com",
            "application-insights.amazonaws.com",
            "events.amazonaws.com",
            "autoscaling.amazonaws.com.cn",
            "events.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchWizardActions0",
      "Effect" : "Allow",
      "Action" : "launchwizard:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SqsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
        "sqs:GetQueueUrl",
        "sqs:AddPermission",
        "sqs:ListQueues",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:LaunchWizard*"
    },
    {
      "Sid" : "CloudWatchActions1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "iam:GetInstanceProfile",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:LaunchWizard*",
        "arn:aws:iam::*:instance-profile/LaunchWizard*"
      ]
```

```
    },
    {
      "Sid" : "EfsActions0",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "route53:ListHostedZones",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:CreateFileSystem",
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Actions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::launchwizard*",
        "arn:aws:s3:::launchwizard*/*",
        "arn:aws:s3:::aws-sap-data-provider/config.properties"
      ]
    },
    {
      "Sid" : "CloudFormationActions2",
      "Effect" : "Allow",
      "Action" : "cloudformation:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "LaunchWizard*"
        }
      }
    },
    {
      "Sid" : "LambdaActions0",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:DeleteBucket",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:LaunchWizard*",
        "arn:aws:s3:::launchwizard*"
      ]
    },
    {
      "Sid" : "DynamodbActions0",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions0",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:LaunchWizard*"
    },
    {
      "Sid" : "SecretsManagerActions1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsMetadata"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SsmActions6",
      "Effect" : "Allow",
      "Action" : "ssm:DeleteOpsMetadata",
      "Resource" : "arn:aws:ssm:*:*:opsmetadata/aws/ssm/LaunchWizard*"
    },
    {
      "Sid" : "SnsActions0",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:LaunchWizard*"
    },
    {
      "Sid" : "FsxActions0",
      "Effect" : "Allow",
      "Action" : [
        "fsx:UntagResource",
        "fsx:TagResource",
        "fsx:DeleteFileSystem",
        "fsx:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/Name" : "LaunchWizard*"
        }
```

```
      }
    },
    {
      "Sid" : "FsxActions1",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : [
            "LaunchWizard*"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions2",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceCatalogActions0",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:CreatePortfolio",
        "servicecatalog:DescribePortfolio",
        "servicecatalog:CreateConstraint",
        "servicecatalog:CreateProduct",
        "servicecatalog:AssociatePrincipalWithPortfolio",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource"
      ],
      "Resource" : [
        "arn:aws:servicecatalog:*:*:*/*",
        "arn:aws:catalog:*:*:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmActions7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EfsActions1",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:UntagResource",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions0",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DescribeLogStreams",
        "logs:UntagResource",
        "logs:TagResource",
```

```
        "logs:CreateLogGroup",
        "logs:DeleteLogStream",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogDelivery",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:ListLogDeliveries"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:LaunchWizard*",
        "arn:aws:logs:*:*:log-group:LaunchWizard*:log-stream:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LogsActions1",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "launchwizard.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FsxActions3",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateStorageVirtualMachine",
        "fsx:CreateVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions4",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxActions5",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteStorageVirtualMachine",
        "fsx:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/LaunchWizard-*/*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "launchwizard.amazonaws.com"
          ]
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexChannelsAccess

Beschreibung: Diese Richtlinie ermöglicht es Kunden, Lex Runtime von Kanälen aus anzurufen

`AmazonLexChannelsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2021, 20:12 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexChannelsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:ListBots"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lex über die AWS-Managementkonsole. Bietet außerdem Zugriff zum Erstellen von Lex Service Linked Roles und zum Erteilen von Lex Berechtigungen zum Aufrufen einer begrenzten Anzahl von Lambda-Funktionen.

`AmazonLexFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLexFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:20 Uhr UTC
- Bearbeitete Zeit: 16. April 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexFullAccessStatement1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:GetPolicy",
        "lambda:ListFunctions",
        "lex:*",
        "polly:DescribeVoices",
        "polly:SynthesizeSpeech",
        "kendra:ListIndices",
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "logs:DescribeLogGroups",
        "s3:GetBucketLocation"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonLex*",
      "Condition" : {
        "StringEquals" : {
          "lambda:Principal" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement4",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement5",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lex.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement6",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement7",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "channels.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement8",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "replication.lexv2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement9",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots",
        "arn:aws:iam::*:role/aws-service-role/channels.lex.amazonaws.com/
AWSServiceRoleForLexChannels",
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*",
```

```
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*",
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ]
    },
    {
      "Sid" : "AmazonLexFullAccessStatement10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lex.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/lexv2.amazonaws.com/
AWSServiceRoleForLexV2Bots*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement12",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/channels.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Channels*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "channels.lexv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonLexFullAccessStatement13",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/replication.lexv2.amazonaws.com/
AWSServiceRoleForLexV2Replication*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lexv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Lex.

`AmazonLexReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLexReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:13 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2024, 16:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonLexReadOnlyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:GetBot",
```

```
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "lex:GetBots",
        "lex:GetBotChannelAssociation",
        "lex:GetBotChannelAssociations",
        "lex:GetBotVersions",
        "lex:GetBuiltinIntent",
        "lex:GetBuiltinIntents",
        "lex:GetBuiltinSlotTypes",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotRecommendation",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:ListBots",
        "lex:ListBotLocales",
        "lex:ListBotAliases",
        "lex:ListBotAliasReplicas",
        "lex:ListBotChannels",
        "lex:ListBotRecommendations",
        "lex:ListBotReplicas",
        "lex:ListBotVersions",
        "lex:ListBotVersionReplicas",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
        "lex:ListRecommendedIntents",
```

```
        "lex:ListSlots",
        "lex:ListSlotTypes",
        "lex:ListTagsForResource",
        "lex:SearchAssociatedTranscripts",
        "lex:ListCustomVocabularyItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexReplicationPolicy

Beschreibung: Ermöglicht Amazon Lex, Lex-Ressourcen in Ihrem Namen regionsübergreifend zu replizieren.

`AmazonLexReplicationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 31. Januar 2024, 23:29 UTC
- Bearbeitete Zeit: 24. Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReplicationServicePolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "lex:BuildBotLocale",
        "lex:ListBotLocales",
        "lex:CreateBotAlias",
        "lex:UpdateBotAlias",
        "lex:DeleteBotAlias",
        "lex:DescribeBotAlias",
        "lex:CreateBotVersion",
        "lex:DeleteBotVersion",
        "lex:DescribeBotVersion",
        "lex:CreateExport",
        "lex:DescribeBot",
        "lex:UpdateExport",
        "lex:DescribeExport",
        "lex:DescribeBotLocale",
        "lex:DescribeIntent",
        "lex:ListIntents",
        "lex:DescribeSlotType",
        "lex:ListSlotTypes",
        "lex:DescribeSlot",
        "lex:ListSlots",
        "lex:DescribeCustomVocabulary",
        "lex:StartImport",
        "lex:DescribeImport",
        "lex:CreateBot",
        "lex:UpdateBot",
```

```
        "lex:DeleteBot",
        "lex:CreateBotLocale",
        "lex:UpdateBotLocale",
        "lex:DeleteBotLocale",
        "lex:CreateIntent",
        "lex:UpdateIntent",
        "lex:DeleteIntent",
        "lex:CreateSlotType",
        "lex:UpdateSlotType",
        "lex:DeleteSlotType",
        "lex:CreateSlot",
        "lex:UpdateSlot",
        "lex:DeleteSlot",
        "lex:CreateCustomVocabulary",
        "lex:UpdateCustomVocabulary",
        "lex:DeleteCustomVocabulary",
        "lex:DeleteBotChannel",
        "lex:ListTagsForResource",
        "lex:TagResource",
        "lex:UntagResource",
        "lex:CreateResourcePolicy",
        "lex:DeleteResourcePolicy",
        "lex:DescribeResourcePolicy",
        "lex:UpdateResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:lex:*:*:bot/*",
        "arn:aws:lex:*:*:bot-alias/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "lex:CreateUploadUrl",
        "lex:ListBots"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReplicationServicePolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lexv2.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexRunBotsOnly

Beschreibung: Ermöglicht den Zugriff auf Amazon Lex Conversational APIs.

`AmazonLexRunBotsOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLexRunBotsOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2017, 23:06 UTC

- Bearbeitete Zeit: 18. August 2021, 00:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLexRunBotsOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lex:PostContent",
        "lex:PostText",
        "lex:PutSession",
        "lex:GetSession",
        "lex:DeleteSession",
        "lex:RecognizeText",
        "lex:RecognizeUtterance",
        "lex:StartConversation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLexV2BotPolicy

Beschreibung: Ermöglicht Lex V2-Bots den Zugriff, um andere AWS Dienste in Ihrem Namen anzurufen.

`AmazonLexV2BotPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2021, 20:10 UTC
- Bearbeitete Zeit: 13. Januar 2021, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonLexV2BotPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutEquipmentFullAccess

Beschreibung: Bietet vollen Zugriff auf den Betrieb von Amazon Lookout for Equipment

`AmazonLookoutEquipmentFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutEquipmentFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. April 2021, 15:52 UTC
- Bearbeitete Zeit: 24. November 2021, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lookoutequipment.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "lookoutequipment.*.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutEquipmentReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Lookout for Equipments

`AmazonLookoutEquipmentReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutEquipmentReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 05. Mai 2021, 16:47 UTC
- Bearbeitete Zeit: 10. November 2022, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutEquipmentReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutequipment:Describe*",
        "lookoutequipment:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutMetricsFullAccess

Beschreibung: Ermöglicht den Zugriff auf alle Aktionen für Amazon Lookout for Metrics

`AmazonLookoutMetricsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutMetricsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Mai 2021, 00:43 UTC
- Bearbeitete Zeit: 7. Mai 2021, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*LookoutMetrics*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "lookoutmetrics.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutMetricsReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf alle schreibgeschützten Aktionen für Amazon Lookout for Metrics

`AmazonLookoutMetricsReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutMetricsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Mai 2021, 00:43 UTC
- Zeit bearbeitet: 4. Januar 2022, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutMetricsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lookoutmetrics:DescribeMetricSet",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:DescribeAnomalyDetectionExecutions",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListTagsForResource",
        "lookoutmetrics:ListAnomalyGroupSummaries",
        "lookoutmetrics:ListAnomalyGroupTimeSeries",
        "lookoutmetrics:ListAnomalyGroupRelatedMetrics",
        "lookoutmetrics:GetAnomalyGroup",
        "lookoutmetrics:GetDataQualityMetrics",
        "lookoutmetrics:GetSampleData",
        "lookoutmetrics:GetFeedback"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Service- und Konsolenabhängigkeiten.

`AmazonLookoutVisionConsoleFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutVisionConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:37 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketFirstUseSetupAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
```

```
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDatasetLabelingToolsAccess",
      "Effect" : "Allow",
      "Action" : [
        "groundtruthlabeling:RunGenerateManifestByCrawlingJob",
        "groundtruthlabeling:AssociatePatchToManifestJob",
        "groundtruthlabeling:DescribeConsoleJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleTagSelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleKmsKeySelectorAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionConsoleReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Service- und Konsolenabhängigkeiten.

`AmazonLookoutVisionConsoleReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutVisionConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:32 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 02:46 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeTrialDetection",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListTrialDetections",
        "lookoutvision:ListModelPackagingJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3BucketSearchAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LookoutVisionConsoleS3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::lookoutvision-*/*"
    },
    {
      "Sid" : "LookoutVisionConsoleDashboardAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonLookoutVisionFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutVisionFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:24 UTC
- Bearbeitete Zeit: 11. Mai 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonLookoutVisionReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Lookout for Vision und bereichsspezifischen Zugriff auf erforderliche Abhängigkeiten.

`AmazonLookoutVisionReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonLookoutVisionReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2021, 19:11 UTC
- Bearbeitete Zeit: 9. Dezember 2021, 03:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonLookoutVisionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LookoutVisionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeProject",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningBatchPredictionsAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, Amazon Machine Learning Learning-Batchvorhersagen anzufordern.

`AmazonMachineLearningBatchPredictionsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningBatchPredictionsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:12 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningBatchPredictionsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateBatchPrediction",
        "machinelearning:DeleteBatchPrediction",
        "machinelearning:DescribeBatchPredictions",
        "machinelearning:GetBatchPrediction",
        "machinelearning:UpdateBatchPrediction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningCreateOnlyAccess

Beschreibung: Bietet Erstellungszugriff für Amazon Machine Learning Learning-Ressourcen ohne Vorhersage.

`AmazonMachineLearningCreateOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningCreateOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:18 Uhr UTC
- Bearbeitete Zeit: 29. Juni 2016, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningCreateOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Add*",
        "machinelearning:Create*",
        "machinelearning:Delete*",
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Machine Learning Learning-Ressourcen.

`AmazonMachineLearningFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:25 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningManageRealTimeEndpointOnlyAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, den Echtzeit-Endpunkt für Amazon Machine Learning Learning-Modelle zu erstellen und zu löschen.

`AmazonMachineLearningManageRealTimeEndpointOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningManageRealTimeEndpointOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 09. April 2015, 17:32 Uhr UTC
- Zeit bearbeitet: 9. April 2015, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningManageRealTimeEndpointOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:CreateRealtimeEndpoint",
        "machinelearning:DeleteRealtimeEndpoint"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Machine Learning Learning-Ressourcen.

`AmazonMachineLearningReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:40 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Describe*",
        "machinelearning:Get*"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningRealTimePredictionOnlyAccess

Beschreibung: Erteilt Benutzern die Erlaubnis, Echtzeitvorhersagen von Amazon Machine Learning anzufordern.

`AmazonMachineLearningRealTimePredictionOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningRealTimePredictionOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. April 2015, 17:44 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMachineLearningRealTimePredictionOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "machinelearning:Predict"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMachineLearningRoleforRedshiftDataSourceV3

Beschreibung: Ermöglicht Machine Learning, Ihre Redshift-Cluster und S3-Staging-Standorte für die Redshift-Datenquelle zu konfigurieren und zu verwenden.

`AmazonMachineLearningRoleforRedshiftDataSourceV3`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonMachineLearningRoleforRedshiftDataSourceV3` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. Juni 2020, 18:00 Uhr UTC
- Bearbeitete Zeit: 24. Juni 2020, 18:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMachineLearningRoleforRedshiftDataSourceV3`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupIngress",
        "redshift:AuthorizeClusterSecurityGroupIngress",
        "redshift:CreateClusterSecurityGroup",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:ModifyCluster",
        "redshift:RevokeClusterSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::amazon-machine-learning*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Macie.

`AmazonMacieFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMacieFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 14:54 UTC
- Bearbeitete Zeit: 1. Juli 2022, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMacieFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "pricing:GetProducts",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieHandshakeRole

Beschreibung: Erteilt die Erlaubnis, die servicebezogene Rolle von Amazon Macie zu erstellen.

`AmazonMacieHandshakeRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMacieHandshakeRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Juni 2018, 15:46 Uhr UTC
- Bearbeitete Zeit: 28. Juni 2018, 15:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieHandshakeRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iam:AWSServiceName" : "macie.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Macie.

`AmazonMacieReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMacieReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Juni 2023, 21:50 UTC
- Bearbeitete Zeit: 15. Juni 2023, 21:50 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMacieReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "macie2:Describe*",
        "macie2:Get*",
        "macie2:List*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:SearchResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieServiceRole

Beschreibung: Gewährt Macie nur Lesezugriff auf Ressourcenabhängigkeiten in Ihrem Konto, um die Datenanalyse zu ermöglichen.

`AmazonMacieServiceRole`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonMacieServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 14:53 Uhr UTC
- Zeit bearbeitet: 14. August 2017, 14:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonMacieServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "s3:Get*",
        "s3:List*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMacieServiceRolePolicy

Beschreibung: Serviceverknüpfte Rolle für Amazon Macie

`AmazonMacieServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juni 2018, 22:17 UTC
- Bearbeitete Zeit: 19. Mai 2022, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMacieServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Managed Blockchain über AWS-Managementkonsole

`AmazonManagedBlockchainConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonManagedBlockchainConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. April 2019, 21:23 Uhr UTC
- Bearbeitete Zeit: 29. April 2019, 21:23 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Managed Blockchain.

`AmazonManagedBlockchainFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonManagedBlockchainFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. April 2019, 21:39 Uhr UTC
- Bearbeitete Zeit: 29. April 2019, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:*"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Managed Blockchain.

`AmazonManagedBlockchainReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonManagedBlockchainReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2019, 18:17 UTC
- Bearbeitete Zeit: 30. April 2019, 18:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonManagedBlockchainReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "managedblockchain:Get*",
        "managedblockchain:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonManagedBlockchainServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon Managed Blockchain verwendet oder verwaltet werden

`AmazonManagedBlockchainServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Januar 2020, 19:51 UTC
- Zeit bearbeitet: 17. Januar 2020, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonManagedBlockchainServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/managedblockchain/*:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMCSFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf Amazon Managed Apache Cassandra Service

`AmazonMCSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMCSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 13:45 Uhr UTC
- Bearbeitete Zeit: 17. April 2020, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/cassandra.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_CassandraTable",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cassandra.application-autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMCSReadOnlyAccess

Beschreibung: Bieten Sie nur Lesezugriff auf Amazon Managed Apache Cassandra Service

`AmazonMCSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMCSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 13:46 UTC
- Bearbeitete Zeit: 17. April 2020, 19:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMCSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMechanicalTurkFullAccess

Beschreibung: Bietet vollen Zugriff auf alles APIs in Amazon Mechanical Turk.

`AmazonMechanicalTurkFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMechanicalTurkFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2015, 19:08 Uhr UTC
- Bearbeitete Zeit: 11. Dezember 2015, 19:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:*"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMechanicalTurkReadOnly

Beschreibung: Bietet APIs in Amazon Mechanical Turk nur Lesezugriff.

`AmazonMechanicalTurkReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMechanicalTurkReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2015, 19:08 Uhr UTC
- Bearbeitete Zeit: 25. September 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMechanicalTurkReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mechanicalturk:Get*",
        "mechanicalturk:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMemoryDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon MemoryDB über die. AWS-Managementkonsole

`AmazonMemoryDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMemoryDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2021, 19:24 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "memorydb:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/memorydb.amazonaws.com/
AWSServiceRoleForMemoryDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "memorydb.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMemoryDBReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon MemoryDB über die. AWS-Managementkonsole

`AmazonMemoryDBReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMemoryDBReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2021, 19:27 UTC
- Bearbeitete Zeit: 8. Oktober 2021, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMemoryDBReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "memorydb:Describe*",
        "memorydb:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsFinancialReportAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Berichte, einschließlich Finanzdaten für alle Anwendungsressourcen.

`AmazonMobileAnalyticsFinancialReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMobileAnalyticsFinancialReportAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFinancialReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mobileanalytics:GetReports",
        "mobileanalytics:GetFinancialReports"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Anwendungsressourcen.

`AmazonMobileAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMobileAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsNon-financialReportAccess

Beschreibung: Bietet Lesezugriff auf Berichte, die keine Finanzberichte sind, für alle Anwendungsressourcen.

`AmazonMobileAnalyticsNon-financialReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMobileAnalyticsNon-financialReportAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsNon-financialReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:GetReports",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMobileAnalyticsWriteOnlyAccess

Beschreibung: Bietet nur Schreibzugriff auf Put-Ereignisdaten für alle Anwendungsressourcen. (Für die SDK-Integration empfohlen)

`AmazonMobileAnalyticsWriteOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMobileAnalyticsWriteOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonMobileAnalyticsWriteOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mobileanalytics:PutEvents",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMonitronFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Monitron

`AmazonMonitronFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMonitronFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2020, 22:40 UTC
- Bearbeitete Zeit: 8. Juni 2022, 16:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMonitronFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitron.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "monitron:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "monitron.*.amazonaws.com"
          ]
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "AWSSSOPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/monitron/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQApiFullAccess

Beschreibung: Bietet vollen Zugriff auf AmazonMQ über unsere API/SDK.

`AmazonMQApiFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonMQApiFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 4. November 2020, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
```

```
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQApiReadOnlyAccess

Beschreibung: Bietet über unsere API/SDK nur Lesezugriff auf AmazonMQ.

`AmazonMQApiReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonMQApiReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Dezember 2018, 20:31 UTC
- Bearbeitete Zeit: 18. Dezember 2018, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQApiReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQFullAccess

Beschreibung: Bietet vollen Zugriff auf AmazonMQ über die. AWS-Managementkonsole

`AmazonMQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMQFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 15:28 Uhr UTC
- Zeit bearbeitet: 4. November 2020, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mq:*",
        "cloudformation:CreateStack",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
```

```
        "ec2:DetachNetworkInterface",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    },
    {
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "mq.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AmazonMQ über die. AWS-Managementkonsole

`AmazonMQReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMQReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2017, 15:30 Uhr UTC
- Bearbeitete Zeit: 28. November 2017, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMQReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mq:Describe*",
        "mq:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMQServiceRolePolicy

Beschreibung: Richtlinie für serviceverknüpfte Rollen für AWS Amazon MQ

`AmazonMQServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. November 2020, 16:07 UTC
- Bearbeitete Zeit: 4. November 2020, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMQServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AMQManaged" : "true"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AMQManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/amazonmq/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKConnectReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon MSK Connect

`AmazonMSKConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMSKConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2021, 10:18 Uhr UTC
- Bearbeitete Zeit: 18. Oktober 2021, 09:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:ListConnectors",
```

```
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeConnector"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:connector/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeCustomPlugin"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:custom-plugin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kafkaconnect:DescribeWorkerConfiguration"
      ],
      "Resource" : [
        "arn:aws:kafkaconnect:*:*:worker-configuration/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKFullAccess

Beschreibung: Gewähren Sie vollen Zugriff auf Amazon MSK und andere erforderliche Berechtigungen für dessen Abhängigkeiten.

`AmazonMSKFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMSKFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2019, 22:07 UTC
- Bearbeitete Zeit: 18. Oktober 2023, 11:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:*",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcAttribute",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "S3:GetBucketPolicy",
        "firehose:TagDeliveryStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "aws:RequestTag/ClusterArn" : "*"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/kafka.amazonaws.com/
AWSServiceRoleForKafka*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "kafka.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMSKReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon MSK

`AmazonMSKReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonMSKReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 14. Januar 2019, 22:28 UTC
- Bearbeitete Zeit: 14. Januar 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonMSKReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "kafka:Describe*",
        "kafka:List*",
        "kafka:Get*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMWAAServerlessServiceRolePolicy

Beschreibung: Bietet Zugriff auf Amazon Airflow Serverless Service, um das Netzwerk für Ihre Workflows zu verwalten und in Ihrem Namen auf andere AWS Dienste zuzugreifen

`AmazonMWAAServerlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2025, 20:34 UTC
- Bearbeitete Zeit: 15. November 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonMWAAServiceRolePolicy

Beschreibung: Die serviceverknüpfte Rolle, die von Amazon Managed Workflows für Apache Airflow verwendet wird.

`AmazonMWAAServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. November 2020, 14:13 Uhr UTC
- Zeit bearbeitet: 17. November 2022, 00:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonMWAAServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:airflow-*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonMWAAManaged" : false
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "AmazonMWAAManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/MWAA"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-LaunchProfileWorker

Beschreibung: Diese Richtlinie gewährt Zugriff auf Ressourcen, die von Nimble Studio Launch Profile-Workern benötigt werden. Hängen Sie diese Richtlinie an EC2 Instanzen an, die von Nimble Studio Builder erstellt wurden.

`AmazonNimbleStudio-LaunchProfileWorker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonNimbleStudio-LaunchProfileWorker` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:47 UTC
- Bearbeitete Zeit: 28. April 2021, 04:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-LaunchProfileWorker`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
```

```
      },
      "Sid" : "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-StudioAdmin

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die mit dem Studio-Administrator verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Fügen Sie diese Richtlinie der Administratorrolle hinzu, die Ihrem Studio zugeordnet ist.

`AmazonNimbleStudio-StudioAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonNimbleStudio-StudioAdmin` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:47 UTC
- Bearbeitete Zeit: 22. September 2023, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioAdmin`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "StudioAdminFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonNimbleStudio-StudioUser

Beschreibung: Diese Richtlinie gewährt Zugriff auf Amazon Nimble Studio-Ressourcen, die mit dem Studio-Benutzer verknüpft sind, und auf zugehörige Studio-Ressourcen in anderen Diensten. Fügen Sie diese Richtlinie der Benutzerrolle hinzu, die Ihrem Studio zugeordnet ist.

`AmazonNimbleStudio-StudioUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonNimbleStudio-StudioUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. April 2021, 04:48 UTC
- Bearbeitete Zeit: 22. September 2023, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonNimbleStudio-StudioUser`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListLaunchProfiles"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:requesterPrincipalId" : "${nimble:principalId}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "nimble:ownedBy" : "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonODBServiceRolePolicy

Beschreibung: Ermöglicht Oracle Database@AWS , AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonODBServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2024, 18:21 UTC
- Bearbeitete Zeit: 29. September 2025, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonODBServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ODB"
          ]
        }
      }
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NM",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EB1",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:ActivateEventSource",
        "events:DescribeEventSource"
      ],
      "Resource" : "arn:aws:events:*:*:event-source/aws.partner/odb*"
    },
    {
      "Sid" : "EB2",
      "Effect" : "Allow",
      "Action" : [
        "events:CreateEventBus",
        "events:DescribeEventBus"
      ],
      "Resource" : "arn:aws:events:*:*:event-bus/aws.partner/odb*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOmicsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Omics und andere erforderliche AWS-Services Funktionen. Diese Richtlinie ermöglicht es dem Benutzer, RAM-Share-Einladungen einzusehen und anzunehmen, um auf Ressourcen zuzugreifen, die sich nicht auf die des Benutzers AWS-Konto beziehen.

`AmazonOmicsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOmicsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Februar 2023, 00:59 UTC

- Bearbeitete Zeit: 24. Februar 2023, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "omics.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "omics.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOmicsReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf Amazon Omics

`AmazonOmicsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOmicsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2022, 04:17 UTC
- Bearbeitete Zeit: 29. November 2022, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOmicsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "omics:Get*",
        "omics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseFullAccess

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen, die den Zugriff auf alle Ressourcen und Abläufe von Amazon One Enterprise ermöglichen.

`AmazonOneEnterpriseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOneEnterpriseFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 04:58 UTC
- Bearbeitete Zeit: 28. November 2023, 04:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseInstallerAccess

Beschreibung: Diese Richtlinie gewährt eingeschränkte Lese- und Schreibberechtigungen, die die Installation und Aktivierung von Geräten ermöglichen.

`AmazonOneEnterpriseInstallerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOneEnterpriseInstallerAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 05:00 UTC
- Bearbeitete Zeit: 28. November 2023, 05:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseInstallerAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "InstallerAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:CreateDeviceActivationQrCode",
        "one:GetDeviceInstance",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceInstances",
        "one:ListSites"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOneEnterpriseReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt allen Amazon One Enterprise-Ressourcen und -Vorgängen nur Leseberechtigungen.

`AmazonOneEnterpriseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOneEnterpriseReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. November 2023, 04:59 UTC
- Bearbeitete Zeit: 28. November 2023, 04:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOneEnterpriseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccessStatementID",
      "Effect" : "Allow",
      "Action" : [
        "one:Get*",
        "one:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchDashboardsServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf Amazon OpenSearch Dashboards Service, um auf andere AWS Dienste zuzugreifen, z. B. in CloudWatch Ihrem Namen

`AmazonOpenSearchDashboardsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Dezember 2023, 19:38 UTC
- Bearbeitete Zeit: 22. Dezember 2023, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchDashboardsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDashboardsServiceRoleAllowedActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSD"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchDirectQueryGlueCreateAccess

Beschreibung: Ermöglicht dem OpenSearch DirectQuery Service den Zugriff auf AWS Glue, APIs um Ressourcen in Ihrem Namen zu erstellen.

`AmazonOpenSearchDirectQueryGlueCreateAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchDirectQueryGlueCreateAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Mai 2024, 12:24 UTC
- Bearbeitungszeit: 6. Mai 2024, 12:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchDirectQueryGlueCreateAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonOpenSearchDirectQueryGlueCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:BatchCreatePartition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionFullAccess

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion, in Ihrem Namen auf andere AWS Dienste zuzugreifen.

`AmazonOpenSearchIngestionFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchIngestionFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. April 2023, 18:11 UTC
- Bearbeitete Zeit: 26. April 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:CreatePipeline",
        "osis:UpdatePipeline",
        "osis:DeletePipeline",
        "osis:StartPipeline",
        "osis:StopPipeline",
        "osis:ListPipelines",
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:ValidatePipeline",
        "osis:GetPipelineBlueprint",
```

```
        "osis:ListPipelineBlueprints",
        "osis:TagResource",
        "osis:UntagResource",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/osis.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchIngestionService",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "osis.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon OpenSearch Ingestion Service

`AmazonOpenSearchIngestionReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchIngestionReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. April 2023, 18:09 UTC
- Bearbeitete Zeit: 26. April 2023, 18:09 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchIngestionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "osis:GetPipeline",
        "osis:GetPipelineChangeProgress",
        "osis:GetPipelineBlueprint",
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchIngestionServiceRolePolicy

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion Service, in Ihrem Namen auf andere AWS Dienste zuzugreifen.

`AmazonOpenSearchIngestionServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2022, 16:49 UTC
- Zeit bearbeitet: 28. August 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchIngestionServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OSISManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServerlessServiceRolePolicy

Beschreibung: Erlauben Sie Amazon OpenSearch Serverless, auf andere AWS Dienste zuzugreifen, z. B. in CloudWatch APIs Ihrem Namen.

`AmazonOpenSearchServerlessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. November 2022, 19:50 UTC
- Bearbeitete Zeit: 25. Juli 2024, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAOSSCloudwatchMetrics",
      "Effect" : "Allow",
```

```
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AOSS"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceCognitoAccess

Beschreibung: Ermöglicht den Zugriff auf den Amazon Cognito Cognito-Konfigurationsservice.

`AmazonOpenSearchServiceCognitoAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchServiceCognitoAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. September 2021, 06:31 UTC
- Bearbeitete Zeit: 20. Dezember 2021, 14:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceCognitoAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:DescribeUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:UpdateUserPoolClient",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:AdminInitiateAuth",
        "cognito-idp:AdminUserGlobalSignOut",
        "cognito-idp:ListUserPoolClients",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:UpdateIdentityPool",
        "cognito-identity:GetIdentityPoolRoles"
      ],
      "Resource" : [
        "arn:aws:cognito-identity:*:*:identitypool/*",
        "arn:aws:cognito-idp:*:*:userpool/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "cognito-identity.amazonaws.com",
            "cognito-identity-us-gov.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "cognito-identity:SetIdentityPoolRoles",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon OpenSearch Service-Konfigurationsservice.

`AmazonOpenSearchServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. September 2021, 05:33 UTC
- Bearbeitete Zeit: 8. September 2021, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon OpenSearch Service-Konfigurationsservice.

`AmazonOpenSearchServiceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonOpenSearchServiceReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. September 2021, 05:38 UTC
- Bearbeitete Zeit: 8. September 2021, 05:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonOpenSearchServiceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:Describe*",
        "es:List*",
        "es:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonOpenSearchServiceRolePolicy

Beschreibung: Erlauben Sie Amazon OpenSearch Service, in Ihrem Namen APIs auf andere AWS Dienste wie EC2 Networking zuzugreifen.

`AmazonOpenSearchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. August 2021, 09:27 UTC
- Bearbeitete Zeit: 27. März 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonOpenSearchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "Stmt1480452973134",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973145",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973144",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973165",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973149",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973150",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "Stmt1480452973154",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973164",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973174",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973184",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates"
      ],
```

```
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:listener/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973194",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973195",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973196",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973197",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/ES",
            "AWS/OpenSearch"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "Stmt1480452973198",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "Stmt1480452973199",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973200",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Stmt1480452973201",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Stmt1480452973202",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sso:PutApplicationAccessScope",
      "Resource" : "arn:aws:sso::*:application/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPersonalizeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Personalize über das AWS-Managementkonsole und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, CloudWatch).

`AmazonPersonalizeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonPersonalizeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Dezember 2018, 22:24 Uhr UTC
- Bearbeitete Zeit: 30. Mai 2019, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonPersonalizeFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "personalize:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*Personalize*",
        "arn:aws:s3:::*personalize*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "personalize.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPollyFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Service und die Ressourcen von Amazon Polly.

`AmazonPollyFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonPollyFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 30. November 2016, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPollyReadOnlyAccess

Beschreibung: Gewährt schreibgeschützten Zugriff auf Amazon Polly Polly-Ressourcen.

`AmazonPollyReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonPollyReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 17. Juli 2018, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPollyReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:DescribeVoices",
        "polly:GetLexicon",
        "polly:GetSpeechSynthesisTask",
        "polly:ListLexicons",
        "polly:ListSpeechSynthesisTasks",
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusConsoleFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS verwaltete Prometheus-Ressourcen in der Konsole AWS

`AmazonPrometheusConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonPrometheusConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:11 Uhr UTC
- Bearbeitete Zeit: 22. Mai 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagValues",
        "tag:GetTagKeys"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace",
        "aps:DescribeWorkspace",
        "aps:UpdateWorkspaceAlias",
        "aps:DeleteWorkspace",
        "aps:ListWorkspaces",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:CreateAlertManagerDefinition",
```

```
        "aps:CreateRuleGroupsNamespace",
        "aps:DeleteAlertManagerDefinition",
        "aps:DeleteRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces",
        "aps:PutAlertManagerDefinition",
        "aps:PutRuleGroupsNamespace",
        "aps:TagResource",
        "aps:UntagResource",
        "aps:CreateLoggingConfiguration",
        "aps:UpdateLoggingConfiguration",
        "aps:DeleteLoggingConfiguration",
        "aps:DescribeLoggingConfiguration",
        "aps:UpdateWorkspaceConfiguration",
        "aps:DescribeWorkspaceConfiguration",
        "aps:CreateQueryLoggingConfiguration",
        "aps:UpdateQueryLoggingConfiguration",
        "aps:DeleteQueryLoggingConfiguration",
        "aps:DescribeQueryLoggingConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS verwaltete Prometheus-Ressourcen

`AmazonPrometheusFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonPrometheusFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:10 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllPrometheusActions",
      "Effect" : "Allow",
      "Action" : [
        "aps:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "aps.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "scraper.aps.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusQueryAccess

Beschreibung: Gewährt Zugriff zum Ausführen von Abfragen für AWS verwaltete Prometheus-Ressourcen

`AmazonPrometheusQueryAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonPrometheusQueryAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2020, 01:02 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusQueryAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:QueryMetrics"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusRemoteWriteAccess

Beschreibung: Gewährt nur Schreibzugriff auf AWS verwaltete Prometheus-Arbeitsbereiche

`AmazonPrometheusRemoteWriteAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonPrometheusRemoteWriteAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2020, 01:04 UTC
- Bearbeitete Zeit: 19. Dezember 2020, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonPrometheusRemoteWriteAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aps:RemoteWrite"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonPrometheusScraperServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon Managed Service für Prometheus Collector verwaltet oder verwendet werden

`AmazonPrometheusScraperServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 26. November 2023, 14:19 UTC
- Bearbeitete Zeit: 26. April 2024, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonPrometheusScraperServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeleteSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/scraper.aps.amazonaws.com/
AWSServiceRoleForAmazonPrometheusScraper*"
    },
    {
      "Sid" : "NetworkDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ENIManagement",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AMPAgentlessScraper"
          ]
        }
      }
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "Null" : {
          "aws:RequestTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "ENIUpdating",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AMPAgentlessScraper" : "false"
        }
      }
    },
    {
      "Sid" : "EKSAccess",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
```

```
    {
      "Sid" : "DeleteEKSAccessEntry",
      "Effect" : "Allow",
      "Action" : "eks:DeleteAccessEntry",
      "Resource" : "arn:aws:eks:*:*:access-entry/*/role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        },
        "ArnLike" : {
          "eks:principalArn" : "arn:aws:iam::*:role/aws-service-role/
scraper.aps.amazonaws.com/AWSServiceRoleForAmazonPrometheusScraper*"
        }
      }
    },
    {
      "Sid" : "APSWriting",
      "Effect" : "Allow",
      "Action" : "aps:RemoteWrite",
      "Resource" : "arn:aws:aps:*:*:workspace/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQDeveloperAccess

Beschreibung: Bietet Entwicklerzugriff, um Interaktionen mit Amazon Q zu ermöglichen

`AmazonQDeveloperAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonQDeveloperAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Juli 2024, 08:35 UTC
- Bearbeitete Zeit: 12. Mai 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQDeveloperAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:StartTroubleshootingResolutionExplanation",
        "q:GetTroubleshootingResults",
```

```
        "q:UpdateTroubleshootingCommandResult",
        "q:GetIdentityMetaData",
        "q:GenerateCodeFromCommands",
        "q:UsePlugin"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQFullAccess

Beschreibung: Bietet vollen Zugriff, um Interaktionen mit Amazon Q zu ermöglichen

`AmazonQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonQFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2023, 16:00 Uhr UTC
- Bearbeitete Zeit: 12. Mai 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAmazonQFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:GetConversation",
        "q:ListConversations",
        "q:UpdateConversation",
        "q:DeleteConversation",
        "q:PassRequest",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
```

```
        "q:GetIdentityMetadata",
        "q:CreateAssignment",
        "q:DeleteAssignment",
        "q:GenerateCodeFromCommands",
        "q:CreatePlugin",
        "q:UpdatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin",
        "q:UsePlugin",
        "q:ListPlugins",
        "q:ListPluginProviders",
        "q:ListTagsForResource",
        "q:UntagResource",
        "q:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCloudControlReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetResource",
        "cloudformation:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "AllowPassRoleToAmazonQ",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "q.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon QLDB über die. AWS-Managementkonsole

`AmazonQLDBConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonQLDBConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:24 Uhr UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:ExecuteStatement",
        "qldb:ShowCatalog",
        "qldb:InsertSampleData",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
```

```
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:ListStreams",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon QLDB über die Service-API.

`AmazonQLDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonQLDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:23 Uhr UTC
- Bearbeitete Zeit: 4. November 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:CreateLedger",
        "qldb:UpdateLedger",
```

```
        "qldb:UpdateLedgerPermissionsMode",
        "qldb:DeleteLedger",
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ExportJournalToS3",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:CancelJournalKinesisStream",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:StreamJournalToKinesis",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:GetBlock",
        "qldb:TagResource",
        "qldb:UntagResource",
        "qldb:ListTagsForResource",
        "qldb:SendCommand",
        "qldb:PartiQLCreateTable",
        "qldb:PartiQLCreateIndex",
        "qldb:PartiQLDropTable",
        "qldb:PartiQLDropIndex",
        "qldb:PartiQLUndropTable",
        "qldb:PartiQLDelete",
        "qldb:PartiQLInsert",
        "qldb:PartiQLUpdate",
        "qldb:PartiQLSelect",
        "qldb:PartiQLHistoryFunction",
        "qldb:PartiQLRedact"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "qldb.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonQLDBReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon QLDB.

`AmazonQLDBReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonQLDBReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. September 2019, 18:19 Uhr UTC
- Bearbeitete Zeit: 2. Juli 2021, 02:17 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonQLDBReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "qldb:ListLedgers",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeJournalKinesisStream",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSBetaServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSBetaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2018, 19:41 UTC
- Bearbeitete Zeit: 7. August 2024, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSBetaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
```

```
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-beta-us-east-1!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-beta-us-
east-1"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomInstanceProfileRolePolicy

Beschreibung: Ermöglicht Amazon RDS Custom, verschiedene Automatisierungsaktionen und Datenbankverwaltungsaufgaben über ein EC2 Instance-Profil auszuführen.

`AmazonRDSCustomInstanceProfileRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSCustomInstanceProfileRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Februar 2024, 17:42 UTC
- Bearbeitete Zeit: 20. März 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSCustomInstanceProfileRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ssmAgentPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssmAgentPermission2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetManifest",
        "ssm:PutConfigurePackageResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssmAgentPermission4",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenControlChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssmAgentPermission5",
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "createEc2SnapshotPermission1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createEc2SnapshotPermission3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createTagForEc2SnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "rdsCustomS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:putObject",
        "s3:getObject",
        "s3:getObjectVersion",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "rdsCustomS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "readSecretsFromCpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "createSecretsOnDpPermission",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "publishCwMetricsPermission",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "rdscustom/rds-custom-sqlserver-agent",
            "RDSCustomForOracle/Agent"
          ]
        }
      }
    },
    {
      "Sid" : "putEventsToEventBusPermission",
      "Effect" : "Allow",
      "Action" : "events:PutEvents",
      "Resource" : "arn:aws:events:*:*:event-bus/default"
    },
    {
      "Sid" : "cwlUploadPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutRetentionPolicy",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:rds-custom-instance-*"
    },
    {
      "Sid" : "sendMessageToSqsQueuePermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:do-not-delete-rds-custom-*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-sqlserver"
        }
      }
    },
    {
      "Sid" : "managePrivateIpOnEniPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : "custom-oracle-rac"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithSecret",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" : [
            "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
            "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
          ]
```

```
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "kmsPermissionWithS3",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-rds-custom-
*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomPreviewServiceRolePolicy

Beschreibung: Rollenrichtlinie für Amazon RDS Custom Preview Service

`AmazonRDSCustomPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:44 UTC
- Zeit bearbeitet: 7. August 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
```

```
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWSRDSCustom*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
```

```
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds-preview.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:preview-rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle"
          ]
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSCustomServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS Custom, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSCustomServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Oktober 2021, 21:39 UTC
- Bearbeitete Zeit: 7. August 2025, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSCustomServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "rdscrc",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ecc1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeImages",
        "ec2:DescribeVpcs",
        "ec2:RegisterImage",
        "ec2:DeregisterImage",
        "ec2:DescribeTags",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
```

```
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ecc2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:TerminateInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RebootInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ecc1scoping3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances1",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:placement-group/*"
      ]
    },
    {
      "Sid" : "eccRunInstances3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac",
```

```
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "eccModifyInstanceAttribute1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ],
          "ec2:Attribute" : "InstanceType"
        }
      }
    },
    {
      "Sid" : "RequireImdsV2",
      "Effect" : "Deny",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringNotEquals" : {
          "ec2:MetadataHttpTokens" : "required"
        },
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccRunInstances3keyPair1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
```

```
        "ec2:DeleteKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccKeyPair2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateKeyPair"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:key-pair/do-not-delete-rds-custom-*",
        "arn:aws:ec2:*:*:key-pair/rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface1",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccNetworkInterface2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "eccNetworkInterface3",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccCreateTag1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "eccCreateTag2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ],
          "ec2:CreateAction" : [
            "CreateKeyPair",
            "RunInstances",
            "CreateNetworkInterface",
            "CreateVolume",
            "CreateSnapshot",
            "CreateSnapshots",
            "CopySnapshot",
            "AllocateAddress",
            "CopyImage"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVolume",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccVolume4snapshot1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
```

```
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot3",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshots",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
```

```
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshot4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver"
          ]
        }
      }
    },
    {
      "Sid" : "eccSnapshotCopySource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
      "Sid" : "eccSnapshotCopyDestination",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/${*}"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "eccAmi1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ]
    },
    {
      "Sid" : "iam1",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "iam2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSRDSCustom*",
        "arn:aws:iam::*:role/service-role/AWSRDSCustom*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "cloudtrail1",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetTrailStatus"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:trail/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "cw1",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "cw2",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:TagResource"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "cw3",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "ssm1",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ssm2",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:GetConnectionStatus",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ssm4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
```

```
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "ssm5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/rds/custom-oracle-rac/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb1",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "eb2",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "eb3",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb4",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:EnableRule",
        "events:DeleteRule",
```

```
        "events:RemoveTargets",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "events:ManagedBy" : [
            "custom.rds.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "eb5",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/do-not-delete-rds-custom-*"
    },
    {
      "Sid" : "secretmanager1",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RestoreSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:do-not-delete-rds-custom-*",
        "arn:aws:secretsmanager:*:*:secret:rds-custom!*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-oracle",
            "custom-sqlserver",
            "custom-oracle-rac"
          ]
        }
      }
    },
    {
      "Sid" : "secretmanager3",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "sqs1",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:TagQueue"
      ],
```

```
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "sqs2",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:SendMessage",
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:DeleteQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:do-not-delete-rds-custom-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSRDSCustom" : [
            "custom-sqlserver",
            "custom-oracle"
          ]
        }
      }
    },
    {
      "Sid" : "servicequota1",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSDataFullAccess

Beschreibung: Ermöglicht vollen Zugriff auf die Verwendung der RDS-Daten APIs, den geheimen Speicher APIs für RDS-Datenbankanmeldeinformationen und das Abfragemanagement der DB-Konsole APIs zur Ausführung von SQL-Anweisungen auf Aurora Serverless-Clustern in der AWS-Konto.

`AmazonRDSDataFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSDataFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2018, 21:29 Uhr UTC
- Bearbeitete Zeit: 20. November 2019, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSDataFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerDbCredentialsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-db-credentials/*"
    },
    {
      "Sid" : "RDSDataServiceAccess",
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory",
        "rds-data:ExecuteSql",
        "rds-data:ExecuteStatement",
        "rds-data:BatchExecuteStatement",
        "rds-data:BeginTransaction",
        "rds-data:CommitTransaction",
        "rds-data:RollbackTransaction",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:GetRandomPassword",
        "tag:GetResources"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSDirectoryServiceAccess

Beschreibung: Erlauben Sie RDS, im Namen des Kunden auf Directory Service Managed AD für domänengebundene SQL Server-DB-Instances zuzugreifen.

`AmazonRDSDirectoryServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSDirectoryServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Februar 2016, 02:02 UTC
- Bearbeitete Zeit: 15. Mai 2019, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSDirectoryServiceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSEnhancedMonitoringRole

Beschreibung: Bietet Zugriff auf Cloudwatch for RDS Enhanced Monitoring

`AmazonRDSEnhancedMonitoringRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSEnhancedMonitoringRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. November 2015, 19:58 Uhr UTC
- Zeit bearbeitet: 11. November 2015, 19:58 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRDSEnhancedMonitoringRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRDSCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
```

```
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:RDS*:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon RDS über die AWS-Managementkonsole.

`AmazonRDSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 17. August 2023, 23:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSFullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:*",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:GetCoipPoolUsage",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish",
```

```
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "outposts:GetOutpostInstanceTypes",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "pi:*",
      "Resource" : [
        "arn:aws:pi:*:*:metrics/rds/*",
        "arn:aws:pi:*:*:perf-reports/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "rds.amazonaws.com",
            "rds.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsFullAccess

Beschreibung: Bietet vollen Zugriff auf RDS Performance Insights über die AWS-Managementkonsole

`AmazonRDSPerformanceInsightsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSPerformanceInsightsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. August 2023, 23:41 UTC
- Bearbeitete Zeit: 20. November 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSPerformanceInsightsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:DescribeDimensionKeys",
        "pi:GetDimensionKeyDetails",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics"
      ],
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsAnalisysReportFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:CreatePerformanceAnalysisReport",
        "pi:GetPerformanceAnalysisReport",
        "pi:ListPerformanceAnalysisReports",
        "pi:DeletePerformanceAnalysisReport"
      ],
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsTaggingFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pi:TagResource",
        "pi:UntagResource",
        "pi:ListTagsForResource"
      ],
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
```

```
    },
    {
      "Sid" : "AmazonRDSDescribeInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:ListTagsForResource",
        "rds:DescribeDBShardGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:shard-group:*"
      ]
    },
    {
      "Sid" : "AmazonCloudWatchReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPerformanceInsightsReadOnly

Beschreibung: Nur-Lese-Richtlinie für RDS Performance Insights

`AmazonRDSPerformanceInsightsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSPerformanceInsightsReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. April 2022, 00:02 UTC
- Zeit bearbeitet: 20. November 2025, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSPerformanceInsightsReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRDSDescribeDBInstances",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "AmazonRDSDescribeDBClusters",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBClusters",
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
```

```
    {
      "Sid" : "AmazonRDSDescribeDBShardGroups",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBShardGroups",
      "Resource" : "arn:aws:rds:*:*:shard-group:*"
    },
    {
      "Sid" : "AmazonRDSListTagsForResource",
      "Effect" : "Allow",
      "Action" : "rds:ListTagsForResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:shard-group:*",
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsDescribeDimensionKeys",
      "Effect" : "Allow",
      "Action" : "pi:DescribeDimensionKeys",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetDimensionKeyDetails",
      "Effect" : "Allow",
      "Action" : "pi:GetDimensionKeyDetails",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetadata",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetadata",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:GetResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceDimensions",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceDimensions",
```

```
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListAvailableResourceMetrics",
      "Effect" : "Allow",
      "Action" : "pi:ListAvailableResourceMetrics",
      "Resource" : "arn:aws:pi:*:*:metrics/rds/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsGetPerformanceAnalysisReport",
      "Effect" : "Allow",
      "Action" : "pi:GetPerformanceAnalysisReport",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListPerformanceAnalysisReports",
      "Effect" : "Allow",
      "Action" : "pi:ListPerformanceAnalysisReports",
      "Resource" : "arn:aws:pi:*:*:perf-reports/rds/*/*"
    },
    {
      "Sid" : "AmazonRDSPerformanceInsightsListTagsForResource",
      "Effect" : "Allow",
      "Action" : "pi:ListTagsForResource",
      "Resource" : "arn:aws:pi:*:*:*/rds/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSPreviewServiceRolePolicy

Beschreibung: Rollenrichtlinie für Amazon RDS Preview Service

`AmazonRDSPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 31. Mai 2018, 18:02 Uhr UTC
- Bearbeitete Zeit: 7. August 2024, 01:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB-Preview",
            "AWS/Neptune-Preview",
            "AWS/RDS-Preview",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*"
      ],
```

```
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds-preview-us-east-2!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds-preview-
us-east-2"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon RDS über die AWS-Managementkonsole.

`AmazonRDSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRDSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 14. April 2023, 12:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRDSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "devops-guru:GetResourceCollection"
      ],
      "Resource" : "*"
    },
    {
      "Action" : [
        "devops-guru:SearchInsights",
        "devops-guru:ListAnomaliesForInsight"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "devops-guru:ServiceNames" : [
            "RDS"
          ]
        },
        "Null" : {
          "devops-guru:ServiceNames" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRDSServiceRolePolicy

Beschreibung: Ermöglicht Amazon RDS, AWS Ressourcen in Ihrem Namen zu verwalten.

`AmazonRDSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Januar 2018, 18:17 UTC
- Bearbeitete Zeit: 1. Juli 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRDSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossRegionCommunication",
      "Effect" : "Allow",
      "Action" : [
        "rds:CrossRegionCommunication"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "Ec2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCoipPoolPermission",
        "ec2:CreateLocalGatewayRouteTablePermission",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteCoipPoolPermission",
        "ec2:DeleteLocalGatewayRouteTablePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTablePermissions",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DisassociateAddress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ]
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/docdb/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "Kinesis",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:CreateStream",
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream",
        "kinesis:SplitShard",
        "kinesis:MergeShards",
        "kinesis:DeleteStream",
        "kinesis:UpdateShardCount"
      ],
      "Resource" : [
        "arn:aws:kinesis:*:*:stream/aws-rds-das-*"
      ]
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/DocDB",
            "AWS/Neptune",
            "AWS/RDS",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:RotateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rds!*"
      ],
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    },
    {
```

```
      "Sid" : "SecretsManagerTags",
      "Effect" : "Allow",
      "Action" : "secretsmanager:TagResource",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rds!*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:rds:primaryDBInstanceArn",
            "aws:rds:primaryDBClusterArn"
          ]
        },
        "StringLike" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "rds"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftAllCommandsFullAccess

Beschreibung: Diese Richtlinie umfasst Berechtigungen zur Ausführung von SQL-Befehlen zum Kopieren, Laden, Entladen, Abfragen und Analysieren von Daten auf Amazon Redshift. Die Richtlinie gewährt auch Berechtigungen zur Ausführung ausgewählter Anweisungen für verwandte Dienste wie Amazon S3, Amazon CloudWatch Logs SageMaker, Amazon oder AWS Glue.

`AmazonRedshiftAllCommandsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftAllCommandsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. November 2021, 00:48 UTC
- Bearbeitete Zeit: 25. November 2021, 02:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftAllCommandsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
```

```
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "SageMaker",
            "/aws/sagemaker/Endpoints",
            "/aws/sagemaker/ProcessingJobs",
            "/aws/sagemaker/TrainingJobs",
            "/aws/sagemaker/TransformJobs"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3:::*redshift*",
        "arn:aws:s3:::*redshift*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "elasticmapreduce:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
```

```
      "Resource" : "arn:aws:lambda:*:*:function:*redshift*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*redshift*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftDataFullAccess

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf Amazon Redshift Redshift-Daten APIs. Diese Richtlinie gewährt auch bereichsbezogenen Zugriff auf andere erforderliche Dienste.

`AmazonRedshiftDataFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftDataFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. September 2020, 19:23 UTC
- Bearbeitete Zeit: 7. April 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftDataFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
```

```
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
      "Sid" : "GetCredentialsForAPIUser",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbname:*/*",
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "GetCredentialsWithFederatedIAMCredentials",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentialsWithIAM",
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*"
    },
    {
      "Sid" : "GetCredentialsForServerless",
      "Effect" : "Allow",
      "Action" : "redshift-serverless:GetCredentials",
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "DenyCreateAPIUser",
      "Effect" : "Deny",
      "Action" : "redshift:CreateClusterUser",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/redshift_data_api_user"
      ]
    },
    {
      "Sid" : "ServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift-data.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift-data.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftFederatedAuthorization

Beschreibung: Dies ist eine ease-of-use Richtlinie für die Ausführung von Abfragen mit Amazon Redshift Federated Authorization

`AmazonRedshiftFederatedAuthorization`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftFederatedAuthorization` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2025, 00:04 Uhr UTC
- Bearbeitete Zeit: 22. November 2025, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFederatedAuthorization`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftFederatedAuthorization",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetUserDefinedFunctions",
        "glue:CreateDatabase",
        "glue:CreateTable",
        "glue:DeleteDatabase",
```

```
        "glue:DeleteTable",
        "glue:UpdateCatalog",
        "glue:UpdateDatabase",
        "glue:UpdateTable",
        "glue:RenameTable",
        "glue:FederateAuthorization"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:FederatedAuthorizationSource" : "Redshift"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftIdentityCenterSetContext",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Redshift über die AWS-Managementkonsole.

`AmazonRedshiftFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 7. Juli 2022, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:*",
        "redshift-serverless:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:DisableAlarmActions",
        "tag:GetResources",
        "tag:UntagResources",
        "tag:GetTagValues",
        "tag:GetTagKeys",
        "tag:TagResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "redshift.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
```

```
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:ResourceTag/RedshiftDataFullAccess" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditor

Beschreibung: Bietet vollen Zugriff auf den Amazon Redshift Query Editor und auf gespeicherte Abfragen über die AWS-Managementkonsole.

`AmazonRedshiftQueryEditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftQueryEditor` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Oktober 2018, 22:50 UTC
- Bearbeitete Zeit: 16. Februar 2021, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditor`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials",
        "redshift:ListSchemas",
        "redshift:ListTables",
        "redshift:ListDatabases",
        "redshift:ExecuteQuery",
        "redshift:FetchResults",
        "redshift:CancelQuery",
        "redshift:DescribeClusters",
        "redshift:DescribeQuery",
        "redshift:DescribeTable",
        "redshift:ViewQueriesFromConsole",
        "redshift:DescribeSavedQueries",
```

```
        "redshift:CreateSavedQuery",
        "redshift:DeleteSavedQueries",
        "redshift:ModifySavedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIPermissions",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "DataAPIIAMSessionPermissionsRestriction",
      "Action" : [
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:ListStatements"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerListPermissions",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerCreateGetPermissions",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/RedshiftQueryOwner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2FullAccess

Beschreibung: Gewährt vollen Zugriff auf die Vorgänge und Ressourcen des Amazon Redshift Query Editor V2. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster, zum Lesen von Schlüsseln und Aliasen in AWS KMS und zum Verwalten der Query Editor V2-Geheimnisse in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftQueryEditorV2FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:06 UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KeyManagementServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*"
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2Permissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2NoSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2, ohne Ressourcen gemeinsam zu nutzen. Der zugewiesene Principal kann nur seine eigenen Ressourcen lesen, aktualisieren und löschen, sie jedoch nicht gemeinsam nutzen. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2NoSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftQueryEditorV2NoSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:18 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2NoSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
```

```
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2ReadSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2 mit begrenzter gemeinsamer Nutzung von Ressourcen. Der bewilligte Principal kann seine eigenen Ressourcen lesen, schreiben und gemeinsam nutzen. Der erteilte Prinzipal kann die mit seinem Team gemeinsam genutzten Ressourcen lesen, sie jedoch nicht aktualisieren. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftQueryEditorV2ReadSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:22 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
```

```
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
```

```
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
```

```
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
```

```
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftQueryEditorV2ReadWriteSharing

Beschreibung: Ermöglicht die Arbeit mit Amazon Redshift Query Editor V2 mit gemeinsamer Nutzung von Ressourcen. Der bewilligte Principal kann seine eigenen Ressourcen lesen, schreiben und gemeinsam nutzen. Der Prinzipal mit den entsprechenden Berechtigungen kann die mit seinem Team geteilten Ressourcen lesen und bearbeiten. Diese Richtlinie gewährt außerdem Zugriff auf andere erforderliche Dienste. Dazu gehören Berechtigungen zum Auflisten der Amazon Redshift Redshift-Cluster und zum Verwalten der Query Editor V2-Geheimnisse des Prinzipals in AWS Secrets Manager.

`AmazonRedshiftQueryEditorV2ReadWriteSharing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftQueryEditorV2ReadWriteSharing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. September 2021, 14:25 Uhr UTC
- Bearbeitete Zeit: 21. Februar 2024, 17:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftQueryEditorV2ReadWriteSharing`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:sqlworkbench!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2NonResourceLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateFolder",
        "sqlworkbench:PutTab",
        "sqlworkbench:BatchDeleteFolder",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:GenerateSession",
        "sqlworkbench:GetAccountInfo",
        "sqlworkbench:GetAccountSettings",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:GetUserWorkspaceSettings",
        "sqlworkbench:PutUserWorkspaceSettings",
        "sqlworkbench:ListConnections",
        "sqlworkbench:ListFiles",
        "sqlworkbench:ListTabs",
        "sqlworkbench:UpdateFolder",
        "sqlworkbench:ListRedshiftClusters",
```

```
        "sqlworkbench:DriverExecute",
        "sqlworkbench:ListTaggedResources",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:ListNotebooks",
        "sqlworkbench:GetSchemaInference",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2CreateOwnedResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateConnection",
        "sqlworkbench:CreateSavedQuery",
        "sqlworkbench:CreateChart",
        "sqlworkbench:CreateNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2OwnerSpecificPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:DeleteChart",
        "sqlworkbench:DeleteConnection",
        "sqlworkbench:DeleteSavedQuery",
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
```

```
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:UpdateFileFolder",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook",
        "sqlworkbench:DeleteNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:CreateNotebookCell",
        "sqlworkbench:DeleteNotebookCell",
        "sqlworkbench:UpdateNotebookCellContent",
        "sqlworkbench:UpdateNotebookCellLayout",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:CreateNotebookVersion",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:DeleteNotebookVersion",
        "sqlworkbench:RestoreNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:ImportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyUserIdPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-resource-owner"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
          "aws:RequestTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
```

```
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TeamReadWriteAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetChart",
        "sqlworkbench:GetConnection",
        "sqlworkbench:GetSavedQuery",
        "sqlworkbench:ListSavedQueryVersions",
        "sqlworkbench:ListTagsForResource",
        "sqlworkbench:UpdateChart",
        "sqlworkbench:UpdateConnection",
        "sqlworkbench:UpdateSavedQuery",
        "sqlworkbench:AssociateConnectionWithTab",
        "sqlworkbench:AssociateQueryWithTab",
        "sqlworkbench:AssociateConnectionWithChart",
        "sqlworkbench:AssociateNotebookWithTab",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:DuplicateNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:ListNotebookVersions",
        "sqlworkbench:GetNotebookVersion",
        "sqlworkbench:CreateNotebookFromVersion",
        "sqlworkbench:ExportNotebook"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2TagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:TagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}",
```

```
          "aws:RequestTag/sqlworkbench-team" : "${aws:PrincipalTag/sqlworkbench-team}"
        }
      }
    },
    {
      "Sid" : "AmazonRedshiftQueryEditorV2UntagOnlyTeamPermissions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:UntagResource",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "sqlworkbench-team"
        },
        "StringEquals" : {
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Redshift über die AWS-Managementkonsole.

`AmazonRedshiftReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRedshiftReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 8. Februar 2024, 00:24 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRedshiftReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRedshiftReadOnlyAccess",
      "Action" : [
        "redshift:Describe*",
        "redshift:ListRecommendations",
        "redshift:ViewQueriesInConsole",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "sns:Get*",
        "sns:List*",
        "cloudwatch:Describe*",
        "cloudwatch:List*",
        "cloudwatch:Get*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRedshiftServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Redshift, AWS Dienste in Ihrem Namen anzurufen

`AmazonRedshiftServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. September 2017, 19:19 Uhr UTC
- Zeit bearbeitet: 19. Februar 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonRedshiftServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2VpcPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PublicAccessCreateEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "PublicAccessReleaseEip",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*"
      ]
    },
    {
      "Sid" : "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CreateSecurityGroupWithTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:ModifySecurityGroupRules",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Redshift" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsOnResources",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSecurityGroup",
            "CreateSubnet",
            "CreateInternetGateway",
            "CreateRouteTable",
            "AllocateAddress"
          ]
        }
      }
    },
    {
      "Sid" : "VPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Redshift-Serverless",
            "AWS/Redshift"
          ]
        }
      }
    },
    {
      "Sid" : "SecretManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:RotateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:redshift!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "redshift",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecretsManagerRandomPassword",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetRandomPassword"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IPV6Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ServiceQuotasToCheckCustomerLimits",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:ec2/L-0263D0A3",
        "arn:aws:servicequotas:*:*:vpc/L-29B6F2EB"
      ]
    },
    {
      "Sid" : "DiscoverRedshiftCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "Bool" : {
          "glue:EnabledForRedshiftAutoDiscovery" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LakeFormationGetMetadataAccessForFederatedCatalogs",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "Bool" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "glue.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionCustomLabelsFullAccess

Beschreibung: Diese Richtlinie spezifiziert Rekognition- und S3-Berechtigungen, die für die Amazon Rekognition Custom Labels-Funktion erforderlich sind.

`AmazonRekognitionCustomLabelsFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonRekognitionCustomLabelsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Januar 2020, 19:18 UTC
- Bearbeitete Zeit: 16. August 2022, 20:20 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionCustomLabelsFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*custom-labels*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CreateProject",
        "rekognition:CreateProjectVersion",
        "rekognition:StartProjectVersion",
        "rekognition:StopProjectVersion",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DeleteProject",
```

```
        "rekognition:DeleteProjectVersion",
        "rekognition:TagResource",
        "rekognition:UntagResource",
        "rekognition:ListTagsForResource",
        "rekognition:CreateDataset",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:UpdateDatasetEntries",
        "rekognition:DistributeDatasetEntries",
        "rekognition:DeleteDataset",
        "rekognition:CopyProjectVersion",
        "rekognition:PutProjectPolicy",
        "rekognition:ListProjectPolicies",
        "rekognition:DeleteProjectPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionFullAccess

Beschreibung: Zugriff auf alle Amazon Rekognition APIs

`AmazonRekognitionFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRekognitionFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 14:40 Uhr UTC
- Bearbeitete Zeit: 30. November 2016, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rekognition:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionReadOnlyAccess

Beschreibung: Zugriff auf alle Read Rekognition APIs

`AmazonRekognitionReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRekognitionReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2016, 14:58 Uhr UTC
- Bearbeitete Zeit: 8. November 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRekognitionReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRekognitionReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:CompareFaces",
        "rekognition:DetectFaces",
```

```
        "rekognition:DetectLabels",
        "rekognition:ListCollections",
        "rekognition:ListFaces",
        "rekognition:SearchFaces",
        "rekognition:SearchFacesByImage",
        "rekognition:DetectText",
        "rekognition:GetCelebrityInfo",
        "rekognition:RecognizeCelebrities",
        "rekognition:DetectModerationLabels",
        "rekognition:GetLabelDetection",
        "rekognition:GetFaceDetection",
        "rekognition:GetContentModeration",
        "rekognition:GetPersonTracking",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetFaceSearch",
        "rekognition:GetTextDetection",
        "rekognition:GetSegmentDetection",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:DescribeProjects",
        "rekognition:DescribeProjectVersions",
        "rekognition:DetectCustomLabels",
        "rekognition:DetectProtectiveEquipment",
        "rekognition:ListTagsForResource",
        "rekognition:ListDatasetEntries",
        "rekognition:ListDatasetLabels",
        "rekognition:DescribeDataset",
        "rekognition:ListProjectPolicies",
        "rekognition:ListUsers",
        "rekognition:SearchUsers",
        "rekognition:SearchUsersByImage",
        "rekognition:GetMediaAnalysisJob",
        "rekognition:ListMediaAnalysisJobs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRekognitionServiceRole

Beschreibung: Ermöglicht Rekognition, AWS Dienste in Ihrem Namen anzurufen.

`AmazonRekognitionServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRekognitionServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. November 2017, 16:52 UTC
- Zeit bearbeitet: 29. November 2017, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonRekognitionServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonRekognition*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetMedia"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53AutoNamingFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2018, 18:40 Uhr UTC
- Bearbeitete Zeit: 18. Januar 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53AutoNamingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2018, 03:02 UTC
- Bearbeitete Zeit: 18. Januar 2018, 03:02 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53AutoNamingRegistrantAccess

Beschreibung: Bietet Zugriff auf Registrantenebene auf Route 53 53-Aktionen zur automatischen Benennung.

`AmazonRoute53AutoNamingRegistrantAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53AutoNamingRegistrantAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. März 2018, 22:33 UTC
- Bearbeitete Zeit: 12. März 2018, 22:33 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53AutoNamingRegistrantAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
```

```
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53DomainsFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Route53-Domänen-Aktionen und ermöglicht die Erstellung von Hosting-Zonen im Rahmen von Domainregistrierungen.

`AmazonRoute53DomainsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53DomainsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:CreateHostedZone",
        "route53domains:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53DomainsReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf die Liste und die Aktionen der Route53-Domänen.

`AmazonRoute53DomainsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53DomainsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53DomainsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53domains:Get*",
        "route53domains:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53FullAccess

Beschreibung: Bietet vollen Zugriff auf alle Amazon Route 53 über die AWS-Managementkonsole.

`AmazonRoute53FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 15. Mai 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:*",
        "route53domains:*",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistributionTenantByDomain",
        "cloudfront:GetConnectionGroup",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRegions",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticbeanstalk:DescribeEnvironments",
        "es:ListDomainNames",
        "es:DescribeDomains",
        "lightsail:GetContainerServices",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/domainnames"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ProfilesFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf Amazon Route 53 53-Profilressourcen.

`AmazonRoute53ProfilesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53ProfilesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2024, 18:30 Uhr UTC
- Bearbeitete Zeit: 27. August 2024, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:AssociateProfile",
        "route53profiles:AssociateResourceToProfile",
        "route53profiles:CreateProfile",
        "route53profiles:DeleteProfile",
        "route53profiles:DisassociateProfile",
        "route53profiles:DisassociateResourceFromProfile",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53profiles:PutProfilePolicy",
        "route53profiles:TagResource",
        "route53profiles:UntagResource",
        "route53profiles:UpdateProfileResourceAssociation",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverRule",
        "ec2:DescribeVpcs",
        "route53:GetHostedZone"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ProfilesReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf Amazon Route 53 53-Profilressourcen.

`AmazonRoute53ProfilesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53ProfilesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. April 2024, 18:29 UTC
- Bearbeitete Zeit: 27. August 2024, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ProfilesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ProfilesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfilePolicy",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallConfig",
        "route53resolver:GetResolverConfig",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverQueryLogConfig"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Route 53 über die AWS-Managementkonsole.

`AmazonRoute53ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 15. November 2016, 21:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:Get*",
        "route53:List*",
        "route53:TestDNSAnswer"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryClusterFullAccess

Beschreibung: Bietet vollen Zugriff auf den Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryClusterFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:37 UTC
- Bearbeitete Zeit: 18. August 2021, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryClusterReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Amazon Route 53 Recovery Cluster

`AmazonRoute53RecoveryClusterReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryClusterReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 17:36 Uhr UTC
- Bearbeitete Zeit: 1. April 2022, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryClusterReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:ListRoutingControls"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryControlConfigFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryControlConfigFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 17:48 Uhr UTC
- Bearbeitete Zeit: 18. August 2021, 17:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "route53-recovery-control-config:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryControlConfigReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Route 53 Recovery Control Config

`AmazonRoute53RecoveryControlConfigReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryControlConfigReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:01 UTC
- Bearbeitete Zeit: 18. Oktober 2023, 17:15 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryControlConfigReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeRoutingControlByName",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryReadinessFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryReadinessFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 16:45 Uhr UTC
- Bearbeitete Zeit: 18. August 2021, 16:45 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53RecoveryReadinessReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Route 53 Recovery Readiness

`AmazonRoute53RecoveryReadinessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53RecoveryReadinessReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2021, 18:11 Uhr UTC
- Bearbeitete Zeit: 09. November 2021, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53RecoveryReadinessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetReadinessCheckResourceStatus",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListCrossAccountAuthorizations",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53-recovery-readiness:ListRules",
        "route53-recovery-readiness:ListTagsForResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53-recovery-readiness:GetArchitectureRecommendations",
        "route53-recovery-readiness:GetCellReadinessSummary"
      ],
      "Resource" : "arn:aws:route53-recovery-readiness::*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ResolverFullAccess

Beschreibung: Vollständige Zugriffsrichtlinie für Route 53 Resolver

`AmazonRoute53ResolverFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53ResolverFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2019, 18:10 Uhr UTC
- Bearbeitete Zeit: 5. August 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AmazonRoute53ResolverFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:*",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonRoute53ResolverReadOnlyAccess

Beschreibung: Schreibgeschützte Richtlinie für Route 53 Resolver

`AmazonRoute53ResolverReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonRoute53ResolverReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2019, 18:11 Uhr UTC
- Bearbeitete Zeit: 5. August 2024, 18:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonRoute53ResolverReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonRoute53ResolverReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:Get*",
        "route53resolver:List*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3FullAccess

Beschreibung: Bietet vollen Zugriff auf alle Buckets über die AWS-Managementkonsole.

`AmazonS3FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 27. September 2021, 20:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:*",
        "s3-object-lambda:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3ObjectLambdaExecutionRolePolicy

Beschreibung: Stellt AWS Lambda-Funktionen Berechtigungen für die Interaktion mit Amazon S3 Object Lambda bereit. Gewährt Lambda außerdem Berechtigungen zum Schreiben in CloudWatch Logs.

`AmazonS3ObjectLambdaExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3ObjectLambdaExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. August 2021, 10:07 UTC

- Bearbeitete Zeit: 18. August 2021, 10:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3ObjectLambdaExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "s3-object-lambda:WriteGetObjectResponse"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3OutpostsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon S3 auf Outposts über die AWS-Managementkonsole.

`AmazonS3OutpostsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3OutpostsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Oktober 2020, 17:26 Uhr UTC
- Bearbeitete Zeit: 2. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3-outposts:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "datasync:ListTasks",
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3OutpostsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon S3 auf Outposts über die AWS-Managementkonsole.

`AmazonS3OutpostsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3OutpostsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Oktober 2020, 18:55 UTC
- Bearbeitete Zeit: 2. Oktober 2020, 18:55 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3OutpostsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3-outposts:Get*",
        "s3-outposts:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:ListTasks",
```

```
        "datasync:ListLocations",
        "datasync:DescribeTask",
        "datasync:DescribeLocation*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:ListOutposts",
        "outposts:GetOutpost"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Buckets über die AWS-Managementkonsole.

`AmazonS3ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 10. August 2023, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:Describe*",
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3TablesFullAccess

Beschreibung: Bietet vollen Zugriff auf alle S3-Tabellen-Buckets.

`AmazonS3TablesFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3TablesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:21 UTC
- Bearbeitete Zeit: 2. Dezember 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToS3TablesReplication",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "replication.s3tables.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3TablesLakeFormationServiceRole

Beschreibung: Diese verwaltete Richtlinie gewährt AWS Lake Formation die Berechtigung, auf alle Tabellen-Buckets, Namespaces und Tabellen innerhalb des Kontos zu reagieren.

`AmazonS3TablesLakeFormationServiceRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmazonS3TablesLakeFormationServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Juni 2025, 19:07 UTC
- Bearbeitete Zeit: 09. Juli 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonS3TablesLakeFormationServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsForS3ListTableBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:ListTableBuckets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:GetTableBucket",
        "s3tables:CreateNamespace",
        "s3tables:GetNamespace",
        "s3tables:ListNamespaces",
        "s3tables:DeleteNamespace",
        "s3tables:DeleteTableBucket",
        "s3tables:CreateTable",
        "s3tables:DeleteTable",
        "s3tables:GetTable",
        "s3tables:ListTables",
        "s3tables:RenameTable",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTableData",
        "s3tables:PutTableData",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3tables:*:*:bucket/*/table/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDescribeKeyAccessPermissionsForS3TablesResources",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3tables.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonS3TablesReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle S3-Tabellen-Buckets.

`AmazonS3TablesReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonS3TablesReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:21 UTC
- Bearbeitete Zeit: 3. Dezember 2024, 15:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonS3TablesReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:Get*",
        "s3tables:List*"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die vom AWS-Service Catalog Service verwendet wird, um Produkte aus dem SageMaker Amazon-Produktportfolio bereitzustellen. Gewährt Berechtigungen für eine Reihe verwandter Dienste CodePipeline CodeBuild CodeCommit, darunter, CloudFormation, Glue usw.

`AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2020, 18:48 Uhr UTC
- Bearbeitete Zeit: 27. September 2025, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerAdmin-ServiceCatalogProductsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPostPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogAPIGatewayPatchPermission",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PATCH"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnMutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "ArnLikeIfExists" : {
          "cloudformation:RoleArn" : [
            "arn:aws:sts::*:assumed-role/AmazonSageMakerServiceCatalog*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCFnTemplatePermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CreateCommit",
        "codecommit:CreateRepository",
        "codecommit:DeleteRepository",
        "codecommit:GetRepository",
        "codecommit:TagResource"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:sagemaker-*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeCommitListPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodePipelinePermission",
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:CreatePipeline",
        "codepipeline:DeletePipeline",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:StartPipelineExecution",
        "codepipeline:TagResource",
        "codepipeline:UpdatePipeline"
      ],
      "Resource" : [
        "arn:aws:codepipeline:*:*:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMUserPermission",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:CreateUserPool",
        "cognito-idp:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:launch-source"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCIAMPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:DeleteGroup",
        "cognito-idp:DeleteUserPool",
        "cognito-idp:DeleteUserPoolClient",
        "cognito-idp:DeleteUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:launch-source" : "*"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogECRPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
```

```
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogFirehosePermission",
      "Effect" : "Allow",
      "Action" : [
        "firehose:CreateDeliveryStream",
        "firehose:DeleteDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "firehose:StartDeliveryStreamEncryption",
        "firehose:StopDeliveryStreamEncryption",
        "firehose:UpdateDestination"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGluePermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:userDefinedFunction/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueClassiferPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateClassifier",
        "glue:DeleteClassifier",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeleteTrigger",
        "glue:DeleteWorkflow",
        "glue:StopCrawler"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueWorkflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateWorkflow"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:workflow/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueJobPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:job/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueCrawlerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:GetCrawler"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:crawler/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogGlueTriggerPermission",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTrigger",
        "glue:GetTrigger"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:trigger/sagemaker-*"
      ]
    },
```

```
    {
      "Sid" : "AmazonSageMakerServiceCatalogPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerServiceCatalog*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLambdaTagPermission",
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogLogGroupPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apigateway/AccessLogs/*",
        "arn:aws:logs:*:*:log-group::log-stream:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadPermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3ReadSagemakerResourcePermission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogS3MutatePermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketAcl",
        "s3:PutBucketNotification",
        "s3:PutBucketPolicy",
```

```
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketTagging",
        "s3:PutObjectTagging"
      ],
      "Resource" : "arn:aws:s3:::sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeWorkteam",
        "sagemaker:CreateCodeRepository",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:DeleteCodeRepository"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
```

```
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "sagemaker:*"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogSageMakerImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateImage",
        "sagemaker:DeleteImage",
        "sagemaker:DescribeImage",
        "sagemaker:UpdateImage",
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:image/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogStepFunctionPermission",
      "Effect" : "Allow",
      "Action" : [
        "states:CreateStateMachine",
        "states:DeleteStateMachine",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeStarPermission",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
```

```
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerServiceCatalogCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasAIServicesAccess

Beschreibung: Ermöglicht Amazon SageMaker Canvas die Nutzung von KI-Services zur Unterstützung einsatzbereiter KI-Lösungen. Diese Richtlinie wird weitere Mutationsberechtigungen für Dienste hinzufügen, sobald Amazon SageMaker Canvas Unterstützung anbietet.

`AmazonSageMakerCanvasAIServicesAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasAIServicesAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2023, 22:36 UTC
- Bearbeitete Zeit: 29. November 2023, 14:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasAIServicesAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Textract",
      "Effect" : "Allow",
      "Action" : [
        "textract:AnalyzeDocument",
        "textract:AnalyzeExpense",
        "textract:AnalyzeID",
        "textract:StartDocumentAnalysis",
        "textract:StartExpenseAnalysis",
        "textract:GetDocumentAnalysis",
        "textract:GetExpenseAnalysis"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "Rekognition",
      "Effect" : "Allow",
      "Action" : [
        "rekognition:DetectLabels",
        "rekognition:DetectText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Comprehend",
      "Effect" : "Allow",
      "Action" : [
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:BatchDetectEntities",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectPiiEntities",
        "comprehend:DetectEntities",
        "comprehend:DetectSentiment",
        "comprehend:DetectDominantLanguage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob",
        "bedrock:CreateProvisionedModelThroughput",
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
```

```
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker",
            "Canvas"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:RequestTag/Canvas" : "true",
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "GetStopAndDeleteBedrockResourcesPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetCustomModel",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:StopModelCustomizationJob",
        "bedrock:DeleteProvisionedModelThroughput"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:model-customization-job/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceTag/Canvas" : "true"
        }
      }
    },
    {
      "Sid" : "FoundationModelPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelCustomizationJob"
```

```
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "BedrockFineTuningPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasBedrockAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Nutzung von Amazon Bedrock in SageMaker Canvas, indem sie Zugriff auf nachgelagerte Dienste wie S3 gewährt.

`AmazonSageMakerCanvasBedrockAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasBedrockAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Februar 2024, 18:37 UTC
- Bearbeitete Zeit: 2. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasBedrockAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3CanvasAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas",
        "arn:aws:s3:::sagemaker-*/Canvas/*"
      ]
    },
    {
      "Sid" : "S3BucketAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDataPrepFullAccess

Beschreibung: Bietet vollen Zugriff auf SageMaker Amazon-Ressourcen und -Operationen für die Datenaufbereitung in Canvas. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM, KMS, RDS, CloudWatch Logs, Redshift, Athena, Glue EventBridge, Secrets Manager). Diese Richtlinie sollte der Ausführungsrolle SageMaker Amazon-Domain/Benutzerprofil zugeordnet werden.

`AmazonSageMakerCanvasDataPrepFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasDataPrepFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2023, 22:56 UTC

- Bearbeitete Zeit: 16. August 2024, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasDataPrepFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerListFeatureGroupOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListFeatureGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerFeatureGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateFeatureGroup",
        "sagemaker:DescribeFeatureGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:feature-group/*"
    },
    {
      "Sid" : "SageMakerProcessingJobOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateProcessingJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:processing-job/*canvas-data-prep*"
```

```
    },
    {
      "Sid" : "SageMakerProcessingJobListOperation",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListProcessingJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPipelineOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribePipeline",
        "sagemaker:CreatePipeline",
        "sagemaker:UpdatePipeline",
        "sagemaker:DeletePipeline",
        "sagemaker:StartPipelineExecution",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:DescribePipelineExecution"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:pipeline/*canvas-data-prep*"
    },
    {
      "Sid" : "KMSListOperations",
      "Effect" : "Allow",
      "Action" : "kms:ListAliases",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSOperations",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListOperations",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
```

```
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgePutOperation",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "EventBridgeTagBasedOperations",
      "Effect" : "Allow",
      "Action" : [
        "events:TagResource"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-data-prep-job" : "true",
          "aws:ResourceTag/sagemaker:is-canvas-data-prep-job" : "true"
        }
      }
    },
    {
      "Sid" : "EventBridgeListTagOperation",
      "Effect" : "Allow",
      "Action" : "events:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:SearchTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "EMROperations",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstanceGroups"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*"
    },
    {
```

```
      "Sid" : "EMRListOperation",
      "Effect" : "Allow",
      "Action" : "elasticmapreduce:ListClusters",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaListDataCatalogOperation",
      "Effect" : "Allow",
      "Action" : "athena:ListDataCatalogs",
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaQueryExecutionOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*"
    },
    {
      "Sid" : "AthenaDataCatalogOperations",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*"
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftArnBasedOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "arn:aws:redshift:*:*:cluster:*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : "redshift:GetClusterCredentials",
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/studio:*"
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessTagResourceOperation",
```

```
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasDirectDeployAccess

Beschreibung: Ermöglicht Amazon SageMaker Canvas das Erstellen, Verwalten und Anzeigen von Endpunktdetails für Endgeräte, die mit Canvas erstellt wurden. Ermöglicht Amazon SageMaker Canvas das Abrufen von Endpunktaufrufmetriken von CloudWatch.

`AmazonSageMakerCanvasDirectDeployAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasDirectDeployAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Oktober 2023, 18:11 UTC
- Bearbeitete Zeit: 6. Oktober 2023, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasDirectDeployAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerEndpointPerms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpoint"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:Canvas*",
        "arn:aws:sagemaker:*:*:canvas*"
      ]
    },
    {
      "Sid" : "ReadCWInvocationMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy

Beschreibung: Diese Richtlinie gewährt Amazon EMR Serverless Berechtigungen für Dienste wie S3, die von Amazon SageMaker Canvas für die Verarbeitung großer Datenmengen verwendet werden.

`AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juli 2024, 00:35 UTC
- Bearbeitungszeit: 27. Juli 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasEMRServerlessExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectOperation",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasForecastAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von SageMaker Canvas mit Amazon Forecast erforderlich sind.

`AmazonSageMakerCanvasForecastAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasForecastAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 24. August 2022, 20:04 UTC
- Bearbeitete Zeit: 24. August 2022, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerCanvasForecastAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/Canvas*",
        "arn:aws:s3:::sagemaker-*/canvas*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasFullAccess

Beschreibung: Bietet vollen Zugriff auf Ressourcen und Abläufe von Amazon SageMaker Canvas. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM, VPC, ECR, CloudWatch Logs, Redshift, Secrets Manager und Forecast). Diese Richtlinie sollte der Ausführungsrolle SageMaker Amazon-Domain/Benutzerprofil zugeordnet werden.

`AmazonSageMakerCanvasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. September 2022, 00:44 UTC
- Bearbeitete Zeit: 16. August 2024, 04:35 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerUserDetailsAndPackageOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListTags",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListEndpoints"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SageMakerPackageGroupOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelPackage"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*"
      ]
    },
    {
      "Sid" : "SageMakerTrainingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:AddTags",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
```

```
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*",
        "arn:aws:sagemaker:*:*:*model-compilation-*"
      ]
    },
    {
      "Sid" : "SageMakerHostingOperations",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteModel",
        "sagemaker:InvokeEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:InvokeEndpointAsync"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:*Canvas*",
        "arn:aws:sagemaker:*:*:*canvas*"
      ]
    },
    {
      "Sid" : "EC2VPCOperation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECROperations",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassOperation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LoggingOperation",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "S3Operations",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:GetBucketCors",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
```

```
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "ReadSageMakerJumpstartArtifacts",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
        "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
      ]
    },
    {
      "Sid" : "S3ListOperations",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueOperations",
      "Effect" : "Allow",
      "Action" : "glue:SearchTables",
      "Resource" : [
        "arn:aws:glue:*:*:table/*/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "SecretsManagerARNBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "SecretManagerTagBasedOperation",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftOperations",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftGetCredentialsOperation",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
```

```
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "ForecastOperations",
      "Effect" : "Allow",
      "Action" : [
        "forecast:CreateExplainabilityExport",
        "forecast:CreateExplainability",
        "forecast:CreateForecastEndpoint",
        "forecast:CreateAutoPredictor",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDataset",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast:CreatePredictorBacktestExportJob",
        "forecast:CreatePredictor",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeExplainability",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeForecastEndpoint",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeDataset",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:GetAccuracyMetrics",
        "forecast:InvokeForecastEndpoint",
        "forecast:GetRecentForecastContext",
        "forecast:DescribePredictor",
        "forecast:TagResource",
        "forecast:DeleteResourceTree"
      ],
      "Resource" : [
        "arn:aws:forecast:*:*:*Canvas*"
      ]
    },
    {
      "Sid" : "RDSOperation",
      "Effect" : "Allow",
      "Action" : "rds:DescribeDBInstances",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMPassOperationForForecast",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "forecast.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "sagemaker",
          "application-autoscaling:scalable-dimension" :
 "sagemaker:variant:DesiredInstanceCount"
        }
      }
    },
    {
      "Sid" : "AsyncEndpointOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "sagemaker:DescribeEndpointConfig"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeScalingOperations",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingActivities"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AutoscalingSageMakerEndpointOperation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AthenaOperation",
      "Action" : [
        "athena:ListTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueOperation",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTables"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuicksightOperation",
      "Action" : [
        "quicksight:ListNamespaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUseOfKeyInAccount",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Source" : "SageMakerCanvas",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessCreateApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:CreateApplication",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListApplicationOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListApplications",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessApplicationOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:UpdateApplication",
        "emr-serverless:StopApplication",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessStartJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:StartJobRun",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessListJobRunOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:ListJobRuns",
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRServerlessJobRunOperations",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetJobRun",
        "emr-serverless:CancelJobRun"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "EMRServerlessTagResourceOperation",
      "Effect" : "Allow",
      "Action" : "emr-serverless:TagResource",
      "Resource" : "arn:aws:emr-serverless:*:*:/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker:is-canvas-resource" : "True",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassOperationForEMRServerless",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerCanvasEMRSExecutionAccess-*",
        "arn:aws:iam::*:role/AmazonSageMakerCanvasEMRSExecutionAccess-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "emr-serverless.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCanvasSMDataScienceAssistantAccess

Beschreibung: Ermöglicht Amazon SageMaker Canvas die Nutzung des SageMaker Data Science Assistant-Service. Der Data Science Assistant verwendet derzeit SageMaker sowohl Amazon als auch Amazon Q Developer, um Benutzeraufforderungen zu verarbeiten.

`AmazonSageMakerCanvasSMDataScienceAssistantAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerCanvasSMDataScienceAssistantAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2024, 14:06 UTC
- Bearbeitete Zeit: 13. Januar 2025, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerCanvasSMDataScienceAssistantAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerDataScienceAssistantAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker-data-science-assistant:SendConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonQDeveloperAccess",
      "Effect" : "Allow",
      "Action" : [
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerClusterInstanceRolePolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die üblicherweise für die Verwendung von Amazon SageMaker Cluster erforderlich sind.

`AmazonSageMakerClusterInstanceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerClusterInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 15:11 UTC
- Bearbeitete Zeit: 29. November 2023, 15:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerClusterInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchLogStreamPublishPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudwatchLogGroupCreationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*"
      ]
    },
    {
      "Sid" : "CloudwatchPutMetricDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "/aws/sagemaker/Clusters"
        }
      }
    },
    {
      "Sid" : "DataRetrievalFromS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SSMConnectivityPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
```

```
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerCoreServiceRolePolicy

Beschreibung: Verwaltete Richtlinie für die serviceverknüpfte Rolle für Amazon SageMaker Core Services

`AmazonSageMakerCoreServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2020, 21:40 Uhr UTC
- Bearbeitete Zeit: 21. Dezember 2020, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerCoreServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:AuthorizedService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerEdgeDeviceFleetPolicy

Beschreibung: Stellt die erforderlichen Berechtigungen bereit, damit SageMaker Edge mithilfe der Standard-Cloud-Verbindung eine Geräteflotte für den Kunden erstellen und verwalten kann.

`AmazonSageMakerEdgeDeviceFleetPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerEdgeDeviceFleetPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Dezember 2020, 16:17 Uhr UTC
- Zeit bearbeitet: 8. Dezember 2020, 16:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerEdgeDeviceFleetPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeviceS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "SageMakerEdgeApis",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SendHeartbeat",
        "sagemaker:GetDeviceRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateIoTRoleAlias",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateRoleAlias",
        "iot:DescribeRoleAlias",
        "iot:UpdateRoleAlias",
        "iot:ListTagsForResource",
        "iot:TagResource"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:rolealias/SageMakerEdge*"
      ]
```

```
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ]
    },
    {
      "Sid" : "CreateIoTRoleAliasIamPermissionsPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*SageMaker*",
        "arn:aws:iam::*:role/*Sagemaker*",
        "arn:aws:iam::*:role/*sagemaker*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "credentials.iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerFeatureStoreAccess

Beschreibung: Stellt die erforderlichen Berechtigungen bereit, um den Offline-Shop für eine SageMaker FeatureStore Amazon-Feature-Gruppe zu aktivieren.

`AmazonSageMakerFeatureStoreAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerFeatureStoreAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 16:24 UTC
- Zeit bearbeitet: 5. Dezember 2022, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFeatureStoreAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*/metadata/*",
        "arn:aws:s3:::*Sagemaker*/metadata/*",
        "arn:aws:s3:::*sagemaker*/metadata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SageMaker über das AWS-Managementkonsole und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, ECR, CloudWatch Logs).

`AmazonSageMakerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 13:07 UTC
- Bearbeitete Zeit: 4. Dezember 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerFullAccess`

Version der Richtlinie

Richtlinienversion: v27 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllNonAdminSageMakerActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*",
        "sagemaker-geospatial:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:partner-app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*",
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowAddTagsForSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    },
    {
      "Sid" : "AllowAddTagsForApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*"
      ]
    },
    {
      "Sid" : "AllowUseOfTrainingPlanResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateCluster",
        "sagemaker:UpdateCluster",
        "sagemaker:DescribeTrainingPlan"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AllowStudioActions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:DescribeSpace",
        "sagemaker:ListSpaces",
        "sagemaker:DescribeApp",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppActionsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*/*/*/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAppActionsForSharedSpaces",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "AllowMutatingActionsOnSharedSpacesWithoutOwner",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "Null" : {
          "sagemaker:OwnerUserProfileArn" : "true"
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
```

```
            "Private",
            "Shared"
          ]
        }
      }
    },
    {
      "Sid" : "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
      "Condition" : {
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
        },
        "StringEquals" : {
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowFlowDefinitionActions",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:GetTemplateSummary",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateRepository",
        "codecommit:GetRepository",
        "codecommit:List*",
        "cognito-idp:AdminAddUserToGroup",
        "cognito-idp:AdminCreateUser",
        "cognito-idp:AdminDeleteUser",
        "cognito-idp:AdminDisableUser",
        "cognito-idp:AdminEnableUser",
        "cognito-idp:AdminRemoveUserFromGroup",
        "cognito-idp:CreateGroup",
        "cognito-idp:CreateUserPool",
        "cognito-idp:CreateUserPoolClient",
        "cognito-idp:CreateUserPoolDomain",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:List*",
        "cognito-idp:UpdateUserPool",
        "cognito-idp:UpdateUserPoolClient",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:CreateRepository",
        "ecr:Describe*",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:StartImageScan",
        "elastic-inference:Connect",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "glue:CreateJob",
        "glue:DeleteJob",
        "glue:GetJob*",
        "glue:GetTable*",
        "glue:GetWorkflowRun",
        "glue:ResetJobBookmark",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:UpdateJob",
        "groundtruthlabeling:*",
        "iam:ListRoles",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery",
```

```
        "robomaker:CreateSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:DeleteSimulationApplication",
        "robomaker:CreateSimulationJob",
        "robomaker:DescribeSimulationJob",
        "robomaker:CancelSimulationJob",
        "secretsmanager:ListSecrets",
        "servicecatalog:Describe*",
        "servicecatalog:List*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProducts",
        "servicecatalog:SearchProvisionedProducts",
        "sns:ListTopics",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECRActions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:SetRepositoryPolicy",
        "ecr:CompleteLayerUpload",
        "ecr:BatchDeleteImage",
        "ecr:UploadLayerPart",
        "ecr:DeleteRepositoryPolicy",
        "ecr:InitiateLayerUpload",
        "ecr:DeleteRepository",
        "ecr:PutImage"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeCommitActions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : [
        "arn:aws:codecommit:*:*:*sagemaker*",
        "arn:aws:codecommit:*:*:*SageMaker*",
```

```
        "arn:aws:codecommit:*:*:*Sagemaker*"
      ]
    },
    {
      "Sid" : "AllowCodeBuildActions",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker*",
        "arn:aws:codebuild:*:*:build/*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowStepFunctionsActions",
      "Action" : [
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:StartExecution",
        "states:StopExecution",
        "states:UpdateStateMachine"
      ],
      "Resource" : [
        "arn:aws:states:*:*:statemachine:*sagemaker*",
        "arn:aws:states:*:*:execution:*sagemaker*:*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "AllowSecretManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
      ]
    },
    {
      "Sid" : "AllowReadOnlySecretManagerActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowServiceCatalogProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ProvisionProduct"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowServiceCatalogTerminateUpdateProvisionProduct",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*",
        "arn:aws:s3:::*aws-glue*"
      ]
    },
    {
      "Sid" : "AllowS3GetObjectWithSageMakerExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/servicecatalog:provisioning" : "true"
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
```

```
        "s3:GetBucketCors",
        "s3:PutBucketCors"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3BucketACL",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowLambdaInvokeFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*"
      ]
    },
    {
      "Sid" : "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowCreateServiceLinkedRoleForRobomaker",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSNSActions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:CreateTopic",
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForSageMakerRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*AmazonSageMaker*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "robomaker.amazonaws.com",
            "states.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToSageMaker",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAthenaActions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowGlueCreateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueUpdateTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:UpdateTable"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/sagemaker_featurestore/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore"
      ]
    },
    {
      "Sid" : "AllowGlueDeleteTable",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*/sagemaker_tmp_*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetTablesAndDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Sid" : "AllowGlueGetAndCreateDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/sagemaker_featurestore",
        "arn:aws:glue:*:*:database/sagemaker_processing",
```

```
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/sagemaker_data_wrangler"
      ]
    },
    {
      "Sid" : "AllowRedshiftDataActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:CancelStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowRedshiftGetClusterCredentials",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
        "arn:aws:redshift:*:*:dbname:*"
      ]
    },
    {
      "Sid" : "AllowListTagsForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "AllowCloudformationListStackResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/SC-*"
    },
    {
      "Sid" : "AllowS3ExpressObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateSession"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*",
        "arn:aws:s3express:*:*:bucket/*aws-glue*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressCreateBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3express:*:*:bucket/*SageMaker*",
        "arn:aws:s3express:*:*:bucket/*Sagemaker*",
        "arn:aws:s3express:*:*:bucket/*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowS3ExpressListBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3express:ListAllMyDirectoryBuckets"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGeospatialExecutionRole

Beschreibung: Diese Richtlinie ermöglicht den Zugriff auf Dienste, die häufig für die Verwendung von SageMaker Geodaten benötigt werden.

`AmazonSageMakerGeospatialExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerGeospatialExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. November 2022, 10:08 UTC
- Bearbeitete Zeit: 10. Mai 2023, 20:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetEarthObservationJob",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:earth-observation-job/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:GetRasterDataCollection",
      "Resource" : "arn:aws:sagemaker-geospatial:*:*:raster-data-collection/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGeospatialFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf Amazon SageMaker Geospatial über das SDK AWS-Managementkonsole und ermöglichen.

`AmazonSageMakerGeospatialFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerGeospatialFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. November 2022, 10:06 UTC
- Zeit bearbeitet: 30. November 2022, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerGeospatialFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "sagemaker-geospatial:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker-geospatial.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerGroundTruthExecution

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste, die für die Ausführung des SageMaker GroundTruth Labeling-Jobs erforderlich sind

`AmazonSageMakerGroundTruthExecution`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerGroundTruthExecution` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Juli 2020, 19:30 Uhr UTC
- Bearbeitete Zeit: 29. April 2022, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerGroundTruthExecution`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CustomLabelingJobs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*GtRecipe*",
        "arn:aws:lambda:*:*:function:*LabelingFunction*",
        "arn:aws:lambda:*:*:function:*SageMaker*",
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*Sagemaker*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*GroundTruth*",
        "arn:aws:s3:::*Groundtruth*",
        "arn:aws:s3:::*groundtruth*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/SageMaker" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StreamingQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : "arn:aws:sqs:*:*:*GroundTruth*"
    },
    {
      "Sid" : "StreamingTopicSubscribe",
      "Effect" : "Allow",
      "Action" : "sns:Subscribe",
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sns:Protocol" : "sqs"
        },
        "StringLike" : {
          "sns:Endpoint" : "arn:aws:sqs:*:*:*GroundTruth*"
        }
      }
    },
    {
      "Sid" : "StreamingTopic",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*GroundTruth*",
        "arn:aws:sns:*:*:*Groundtruth*",
        "arn:aws:sns:*:*:*groundTruth*",
        "arn:aws:sns:*:*:*groundtruth*",
        "arn:aws:sns:*:*:*SageMaker*",
        "arn:aws:sns:*:*:*Sagemaker*",
        "arn:aws:sns:*:*:*sageMaker*",
        "arn:aws:sns:*:*:*sagemaker*"
      ]
    },
    {
      "Sid" : "StreamingTopicUnsubscribe",
      "Effect" : "Allow",
      "Action" : [
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WorkforceVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ec2:VpceServiceName" : [
            "*sagemaker-task-resources*",
            "aws.sagemaker*labeling*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerHyperPodObservabilityAdminAccess

Beschreibung: Diese Richtlinie bietet Administratorrechte, die für die Einrichtung von SageMaker HyperPod Observability erforderlich sind. Es ermöglicht den Zugriff auf Amazon Managed Prometheus, Amazon Managed Grafana und EKS Addons. Die Richtlinie beinhaltet auch einen umfassenden Zugriff auf Grafana-HTTP APIs ServiceAccountTokens über alle Amazon Managed Grafana-Workspaces in Ihrem Konto.

`AmazonSageMakerHyperPodObservabilityAdminAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerHyperPodObservabilityAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Juli 2025, 14:37 UTC
- Bearbeitete Zeit: 21. August 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodObservabilityAdminAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrometheusCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusTagsAccess",
      "Effect" : "Allow",
      "Action" : "aps:TagResource",
      "Resource" : [
        "arn:aws:aps:*:*:/workspaces",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "PrometheusDescribeAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aps:DescribeWorkspace"
      ],
      "Resource" : "arn:aws:aps:*:*:workspace/*"
    },
    {
      "Sid" : "PrometheusListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrometheusAlertsRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:CreateAlertManagerDefinition",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeRuleGroupsNamespace",
        "aps:ListRuleGroupsNamespaces"
      ],
      "Resource" : [
        "arn:aws:aps:*:*:workspace/*",
        "arn:aws:aps:*:*:rulegroupsnamespace/*/HyperPodObservabilityNamespace"
      ]
    },
    {
      "Sid" : "PrometheusCreateRuleGroupAccess",
      "Effect" : "Allow",
      "Action" : "aps:CreateRuleGroupsNamespace",
      "Resource" : "arn:aws:aps:*:*:rulegroupsnamespace/*/
HyperPodObservabilityNamespace",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaCreateWorkspaceAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "grafana:CreateWorkspace"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaTagsAccess",
      "Effect" : "Allow",
      "Action" : "grafana:TagResource",
      "Resource" : "arn:aws:grafana:*:*:/workspaces",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "GrafanaListAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:ListWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaServiceAccountAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:CreateWorkspaceApiKey",
        "grafana:CreateWorkspaceServiceAccount",
        "grafana:CreateWorkspaceServiceAccountToken",
        "grafana:ListWorkspaceServiceAccounts",
```

```
        "grafana:ListWorkspaceServiceAccountTokens",
        "grafana:DeleteWorkspaceServiceAccountToken"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces/*"
    },
    {
      "Sid" : "IAMGrafanaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityGrafanaAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "grafana.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMEKSPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "pods.eks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerHyperPodObservabilityAddonAccess-*"
```

```
      ]
    },
    {
      "Sid" : "HyperPodClusterAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListClusters",
        "sagemaker:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DeleteAddon",
        "eks:UpdateAddon",
        "eks:DescribeAddon"
      ],
      "Resource" : "arn:aws:eks:*:*:addon/*/amazon-sagemaker-hyperpod-observability/*"
    },
    {
      "Sid" : "EKSAddonDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeAddonConfiguration",
        "eks:DescribeAddonVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSAddonPodIdentityAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribePodIdentityAssociation",
        "eks:DeletePodIdentityAssociation",
        "eks:UpdatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:podidentityassociation/*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "EKSListDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListAddons",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "EKSCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAddon",
        "eks:CreatePodIdentityAssociation"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true"
        }
      }
    },
    {
      "Sid" : "EKSTagsAccess",
      "Effect" : "Allow",
      "Action" : "eks:TagResource",
      "Resource" : [
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:addon/*/*/*",
        "arn:aws:eks:*:*:podidentityassociation/*/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SageMaker"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SageMaker" : "true",
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SSOAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:CreateManagedApplicationInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerHyperPodServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Amazon Berechtigungen SageMaker HyperPod für verwandte AWS Dienste wie Amazon EKS, Amazon CloudWatch usw.

`AmazonSageMakerHyperPodServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. September 2024, 17:04 UTC
- Bearbeitete Zeit: 6. September 2024, 17:04 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerHyperPodServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EKSClusterDescribePermissions",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchLogStreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/Clusters/*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerHyperPodTrainingOperatorAccess

Beschreibung: Diese Richtlinie bietet Administratorberechtigungen, die für die Einrichtung des SageMaker HyperPod Schulungsoperators erforderlich sind. Es ermöglicht den Zugriff auf Amazon SageMaker HyperPod - und EKS-Add-Ons. Die Richtlinie beinhaltet Berechtigungen zur Beschreibung der SageMaker HyperPod Ressourcen in Ihrem Konto.

`AmazonSageMakerHyperPodTrainingOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerHyperPodTrainingOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. August 2025, 17:04 UTC

- Bearbeitete Zeit: 19. August 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerHyperPodTrainingOperatorAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDescribeClusterNodeOnHyperPodClusters",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeClusterNode",
      "Resource" : "arn:aws:sagemaker:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SageMaker" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerMechanicalTurkAccess

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Amazon Augmented FlowDefinition AI-Ressourcen für jedes Workteam.

`AmazonSageMakerMechanicalTurkAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerMechanicalTurkAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 16:19 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerMechanicalTurkAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerModelGovernanceUseAccess

Beschreibung: Diese AWS verwaltete Richtlinie gewährt Berechtigungen, die für die Nutzung aller Amazon SageMaker Governance-Funktionen erforderlich sind. Die Richtlinie bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS).

`AmazonSageMakerModelGovernanceUseAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerModelGovernanceUseAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2022, 08:58 UTC
- Bearbeitete Zeit: 4. Juni 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelGovernanceUseAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSMMonitoringModelCards",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:UpdateMonitoringAlert",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:ListMonitoringAlertHistory",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:CreateModelCard",
        "sagemaker:DescribeModelCard",
        "sagemaker:UpdateModelCard",
        "sagemaker:DeleteModelCard",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelCardVersions",
        "sagemaker:CreateModelCardExportJob",
        "sagemaker:DescribeModelCardExportJob",
        "sagemaker:ListModelCardExportJobs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSMTrainingModelsSearchTags",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:ListModels",
        "sagemaker:DescribeModel",
        "sagemaker:Search",
```

```
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "sagemaker:ListTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3Actions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:CreateBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowS3ListActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerModelRegistryFullAccess

Beschreibung: Dies ist eine neue verwaltete Richtlinie für Model Registry in Sagemaker. Bei dieser Richtlinie handelt es sich um eine eigenständige Richtlinie, die an die Benutzerrolle angehängt werden kann, um auf Funktionen im Zusammenhang mit Model Registry in Sagemaker zuzugreifen.

`AmazonSageMakerModelRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerModelRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2023, 05:20 UTC
- Bearbeitungszeit: 6. Juni 2024, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerModelRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeAction",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:ListAssociations",
        "sagemaker:ListArtifacts",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackages",
        "sagemaker:Search",
        "sagemaker:GetSearchSuggestions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistrySageMakerWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteTags",
        "sagemaker:UpdateModelPackage"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AmazonSageMakerModelRegistryS3GetPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryS3ListPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryTagReadPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : "sagemaker:collection"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker:collection" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceKMSPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/sagemaker" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerNotebooksServiceRolePolicy

Beschreibung: Verwaltete Richtlinie für Service Linked Role für Amazon SageMaker Notebooks

`AmazonSageMakerNotebooksServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Oktober 2019, 20:27 UTC
- Bearbeitete Zeit: 10. Dezember 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSageMakerNotebooksServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFSxDescribe",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowSageMakerDeleteApp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DeleteApp"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:app/*"
    },
    {
      "Sid" : "AllowEFSAccessPointCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateAccessPoint",
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*",
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSAccessPointDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DeleteAccessPoint"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:access-point/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSCreation",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:CreateFileSystem",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/ManagedByAmazonSageMakerResource" : "*"
        }
```

```
      }
    },
    {
      "Sid" : "AllowEFSMountWithDeletion",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:CreateMountTarget",
        "elasticfilesystem:DeleteFileSystem",
        "elasticfilesystem:DeleteMountTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEFSDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEFSTagging",
      "Effect" : "Allow",
      "Action" : "elasticfilesystem:TagResource",
      "Resource" : [
        "arn:aws:elasticfilesystem:*:*:access-point/*",
        "arn:aws:elasticfilesystem:*:*:file-system/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowEC2Tagging",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowEC2Operations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2AuthZ",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/ManagedByAmazonSageMakerResource" : "*"
        }
      }
    },
    {
      "Sid" : "AllowIdcOperations",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sso:CreateManagedApplicationInstance",
        "sso:DeleteManagedApplicationInstance",
        "sso:GetManagedApplicationInstance"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowSagemakerProfileCreation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:CreateUserProfile",
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSagemakerSpaceOperationsForCanvasManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:DescribeSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*"
    },
    {
      "Sid" : "AllowSagemakerAddTagsForAppManagedSpaces",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*/CanvasManagedSpace-*",
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : "CreateSpace"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerAppsFullAccess

Beschreibung: Ermöglicht Benutzern von SageMaker Amazon-Partner-Apps, auf Anwendungen zuzugreifen, verfügbare Anwendungen aufzulisten, das Anwendungsweb UIs zu starten und eine Verbindung über das Anwendungs-SDK herzustellen.

`AmazonSageMakerPartnerAppsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerPartnerAppsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Januar 2025, 18:37 UTC
- Bearbeitete Zeit: 17. Januar 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerPartnerListAppsPermission",
      "Effect" : "Allow",
```

```
      "Action" : "sagemaker:ListPartnerApps",
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonSageMakerPartnerAppsPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:DescribePartnerApp",
        "sagemaker:CallPartnerAppApi"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:sagemaker:*:*:partner-app/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceR

Beschreibung: Servicerollenrichtlinie, die AWS APIGateway vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Lambda und andere.

`AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 01. August 2023, 15:06 UTC
- Bearbeitete Zeit: 1. August 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:sagemaker-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sagemaker:InvokeEndpoint",
      "Resource" : "arn:aws:sagemaker:*:*:endpoint/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServi

Beschreibung: Servicerollenrichtlinie, die AWS CloudFormation vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste, einschließlich Lambda APIGateway und anderen.

`AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. August 2023, 15:06 UTC
- Bearbeitete Zeit: 1. August 2023, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsCloudFormationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsLambdaRole"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsApiGatewayRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "apigateway.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:ListTags",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PublishLayerVersion",
        "lambda:GetLayerVersion",
        "lambda:DeleteLayerVersion",
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:sagemaker-*",
        "arn:aws:lambda:*:*:function:sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
```

```
          "aws:ResourceTag/sagemaker:partner" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:project-name" : "false",
          "aws:ResourceTag/sagemaker:partner" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name",
            "sagemaker:partner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*/lambda-auth-code/layer.zip"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRoleP

Beschreibung: Richtlinie für Servicerollen, die von AWS Lambda in den AWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Secrets Manager und andere.

`AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. August 2023, 15:05 UTC
- Bearbeitete Zeit: 1. August 2023, 15:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerPartnerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:partner" : false
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerPipelinesIntegrations

Beschreibung: Diese von Amazon Managed Policy gewährte Berechtigungen, die üblicherweise für die Verwendung mit Callback-Schritten und Lambda-Schritten in SageMaker Model Building-Pipelines benötigt werden. Sie wird dem hinzugefügt AmazonSageMaker — ExecutionRole das kann bei der Einrichtung von Studio erstellt werden. SageMaker Sie kann auch an jede andere Rolle angehängt werden, die für die Erstellung oder Ausführung von Pipelines verwendet wird.

`AmazonSageMakerPipelinesIntegrations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerPipelinesIntegrations` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Juli 2021, 16:35 UTC
- Bearbeitete Zeit: 17. Februar 2023, 21:28 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerPipelinesIntegrations`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*sagemaker*",
        "arn:aws:lambda:*:*:function:*sageMaker*",
```

```
        "arn:aws:lambda:*:*:function:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:*sagemaker*",
        "arn:aws:sqs:*:*:*sageMaker*",
        "arn:aws:sqs:*:*:*SageMaker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "elasticmapreduce.amazonaws.com",
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRStepStatusUpdateRule",
        "arn:aws:events:*:*:rule/SageMakerPipelineExecutionEMRClusterStatusUpdateRule"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:ListSteps"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerQuickSightVPCPolicy

Beschreibung: Diese Richtlinie wird von SageMaker Unified Studios verwendet, um VPC-bezogene Ressourcen für zu erstellen QuickSight

`AmazonSageMakerQuickSightVPCPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerQuickSightVPCPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 03. Juni 2025, 17:37 UTC
- Bearbeitete Zeit: 03. Juni 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerQuickSightVPCPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageQuickSightVPCConnection",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListVPCConnections",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcconnection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeQuickSightVPCConnectionEC2Resources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightEC2NetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerReadOnly

Beschreibung: Ermöglicht Lesezugriff auf Amazon SageMaker über das SDK AWS-Managementkonsole und.

`AmazonSageMakerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 13:07 UTC
- Bearbeitete Zeit: 1. Dezember 2021, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerReadOnly`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Describe*",
```

```
        "sagemaker:List*",
        "sagemaker:BatchGetMetrics",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:BatchGetRecord",
        "sagemaker:GetRecord",
        "sagemaker:Search",
        "sagemaker:QueryLineage",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:GetModelPackageGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "aws-marketplace:ViewSubscriptions",
        "cloudwatch:DescribeAlarms",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "ecr:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePoli

Beschreibung: Servicerollenrichtlinie, die AWS APIGateway vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter CloudWatch Logs und andere.

`AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2022, 04:25 UTC
- Bearbeitete Zeit: 25. März 2022, 04:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsApiGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apigateway/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCloudformationServiceRoleP

Beschreibung: Servicerollenrichtlinie, die AWS CloudFormation vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste, darunter auch für andere SageMaker .

`AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2022, 04:26 UTC
- Bearbeitete Zeit: 25. März 2022, 04:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCloudformationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
```

```
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
```

```
            "sagemaker:DeleteTags",
            "sagemaker:DeleteTrial",
            "sagemaker:DeleteTrialComponent",
            "sagemaker:DeleteUserProfile",
            "sagemaker:DeleteWorkforce",
            "sagemaker:DeleteWorkteam",
            "sagemaker:DeregisterDevices",
            "sagemaker:DescribeAction",
            "sagemaker:DescribeAlgorithm",
            "sagemaker:DescribeApp",
            "sagemaker:DescribeAppImageConfig",
            "sagemaker:DescribeArtifact",
            "sagemaker:DescribeAutoMLJob",
            "sagemaker:DescribeCodeRepository",
            "sagemaker:DescribeCompilationJob",
            "sagemaker:DescribeContext",
            "sagemaker:DescribeDataQualityJobDefinition",
            "sagemaker:DescribeDevice",
            "sagemaker:DescribeDeviceFleet",
            "sagemaker:DescribeDomain",
            "sagemaker:DescribeEdgePackagingJob",
            "sagemaker:DescribeEndpoint",
            "sagemaker:DescribeEndpointConfig",
            "sagemaker:DescribeExperiment",
            "sagemaker:DescribeFeatureGroup",
            "sagemaker:DescribeFlowDefinition",
            "sagemaker:DescribeHumanLoop",
            "sagemaker:DescribeHumanTaskUi",
            "sagemaker:DescribeHyperParameterTuningJob",
            "sagemaker:DescribeImage",
            "sagemaker:DescribeImageVersion",
            "sagemaker:DescribeInferenceRecommendationsJob",
            "sagemaker:DescribeLabelingJob",
            "sagemaker:DescribeLineageGroup",
            "sagemaker:DescribeModel",
            "sagemaker:DescribeModelBiasJobDefinition",
            "sagemaker:DescribeModelExplainabilityJobDefinition",
            "sagemaker:DescribeModelPackage",
            "sagemaker:DescribeModelPackageGroup",
            "sagemaker:DescribeModelQualityJobDefinition",
            "sagemaker:DescribeMonitoringSchedule",
            "sagemaker:DescribeNotebookInstance",
            "sagemaker:DescribeNotebookInstanceLifecycleConfig",
            "sagemaker:DescribePipeline",
```

```
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
```

```
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
```

```
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
```

```
        "sagemaker:UpdateWorkteam"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die AWS CodeBuild vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste CodePipeline, einschließlich CodeBuild und anderer.

`AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. März 2022, 04:27 UTC
- Bearbeitete Zeit: 27. September 2025, 04:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerServiceCatalogProductsCodeBuildServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodeBuildECRReadPermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeImageReplicationStatus",
        "ecr:DescribeRepositories",
        "ecr:DescribeImageReplicationStatus",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildECRWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildPassRoletPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsEventsRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodePipelineRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole",
```

```
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCodeBuildRole",
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com",
            "codepipeline.amazonaws.com",
            "cloudformation.amazonaws.com",
            "codebuild.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*"
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodeBuildS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
```

```
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
```

```
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
```

```
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
```

```
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
```

```
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
```

```
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:model-package/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
```

```
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodeBuildCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePo

Beschreibung: Servicerollenrichtlinie, die AWS CodePipeline vom SageMaker Produktportfolio für AWS ServiceCatalog bereitgestellte Produkte von Amazon verwendet wird. Gewährt Berechtigungen für eine Teilmenge verwandter Dienste CodePipeline, einschließlich CodeBuild und anderer.

`AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 27. September 2025, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsCodePipelineServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCFnTagPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sagemaker-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "sagemaker:project-name"
          ]
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineS3Permission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
```

```
      "Sid" : "AmazonSageMakerCodePipelinePassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsCloudformationRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "arn:aws:codebuild:*:*:project/sagemaker-*",
        "arn:aws:codebuild:*:*:build/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeCommitPermission",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:CancelUploadArchive",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:UploadArchive"
      ],
      "Resource" : "arn:aws:codecommit:*:*:sagemaker-*"
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeStarConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
```

```
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerCodePipelineCodeConnectionPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codestar-connections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/sagemaker" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy

Beschreibung: Servicerollenrichtlinie, die von den AWS CloudWatch Events innerhalb des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Erteilt Berechtigungen für eine Teilmenge verwandter Dienste, darunter auch für andere CodePipeline .

`AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:53 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "codepipeline:StartPipelineExecution",
      "Resource" : "arn:aws:codepipeline:*:*:sagemaker-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Firehose im Rahmen des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Firehose und andere.

`AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:54 UTC
- Bearbeitete Zeit: 22. Februar 2022, 09:54 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsFirehoseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/sagemaker-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Glue im Rahmen des AWS ServiceCatalog bereitgestellten SageMaker Produktportfolios von Amazon verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter Glue, S3 und andere.

`AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Februar 2022, 09:51 UTC
- Bearbeitete Zeit: 26. August 2022, 19:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsGlueServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeletePartition",
        "glue:DeleteTable",
```

```
        "glue:DeleteTableVersion",
        "glue:GetDatabase",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:SearchTables",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:database/sagemaker-*",
        "arn:aws:glue:*:*:table/sagemaker-*",
        "arn:aws:glue:*:*:tableVersion/sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/glue/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy

Beschreibung: Richtlinie für Servicerollen, die von AWS Lambda in den AWS ServiceCatalog bereitgestellten Produkten aus dem SageMaker Amazon-Produktportfolio verwendet wird. Gewährt Berechtigungen für eine Reihe verwandter Dienste, darunter ECR, S3 und andere.

`AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. April 2022, 16:34 UTC
- Bearbeitungszeit: 11. Juni 2024, 18:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSageMakerServiceCatalogProductsLambdaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSageMakerLambdaECRPermission",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecr:DescribeImages",
        "ecr:BatchDeleteImage",
        "ecr:CompleteLayerUpload",
        "ecr:CreateRepository",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaEventBridgePermission",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3BucketPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutBucketCors"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
```

```
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaS3ObjectPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*",
        "arn:aws:s3:::sagemaker-*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaSageMakerPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:AssociateTrialComponent",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchGetRecord",
        "sagemaker:BatchPutMetrics",
        "sagemaker:CreateAction",
        "sagemaker:CreateAlgorithm",
        "sagemaker:CreateApp",
        "sagemaker:CreateAppImageConfig",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCodeRepository",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateContext",
        "sagemaker:CreateDataQualityJobDefinition",
        "sagemaker:CreateDeviceFleet",
        "sagemaker:CreateDomain",
        "sagemaker:CreateEdgePackagingJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
```

```
        "sagemaker:CreateExperiment",
        "sagemaker:CreateFeatureGroup",
        "sagemaker:CreateFlowDefinition",
        "sagemaker:CreateHumanTaskUi",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateImage",
        "sagemaker:CreateImageVersion",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateLabelingJob",
        "sagemaker:CreateLineageGroupPolicy",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelBiasJobDefinition",
        "sagemaker:CreateModelExplainabilityJobDefinition",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateModelQualityJobDefinition",
        "sagemaker:CreateMonitoringSchedule",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateProject",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateTrial",
        "sagemaker:CreateTrialComponent",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateWorkforce",
        "sagemaker:CreateWorkteam",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteAlgorithm",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteAppImageConfig",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteCodeRepository",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteDataQualityJobDefinition",
        "sagemaker:DeleteDeviceFleet",
        "sagemaker:DeleteDomain",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
```

```
        "sagemaker:DeleteExperiment",
        "sagemaker:DeleteFeatureGroup",
        "sagemaker:DeleteFlowDefinition",
        "sagemaker:DeleteHumanLoop",
        "sagemaker:DeleteHumanTaskUi",
        "sagemaker:DeleteImage",
        "sagemaker:DeleteImageVersion",
        "sagemaker:DeleteLineageGroupPolicy",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelBiasJobDefinition",
        "sagemaker:DeleteModelExplainabilityJobDefinition",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteModelPackageGroupPolicy",
        "sagemaker:DeleteModelQualityJobDefinition",
        "sagemaker:DeleteMonitoringSchedule",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteProject",
        "sagemaker:DeleteRecord",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteTrial",
        "sagemaker:DeleteTrialComponent",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DeleteWorkforce",
        "sagemaker:DeleteWorkteam",
        "sagemaker:DeregisterDevices",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDevice",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEdgePackagingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
```

```
        "sagemaker:DescribeExperiment",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanLoop",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeLineageGroup",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeSubscribedWorkteam",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrial",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkforce",
        "sagemaker:DescribeWorkteam",
        "sagemaker:DisableSagemakerServicecatalogPortfolio",
        "sagemaker:DisassociateTrialComponent",
        "sagemaker:EnableSagemakerServicecatalogPortfolio",
        "sagemaker:GetDeviceFleetReport",
        "sagemaker:GetDeviceRegistration",
        "sagemaker:GetLineageGroupPolicy",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:GetRecord",
        "sagemaker:GetSagemakerServicecatalogPortfolioStatus",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
```

```
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListCompilationJobs",
        "sagemaker:ListContexts",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDevices",
        "sagemaker:ListDomains",
        "sagemaker:ListEdgePackagingJobs",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanLoops",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceRecommendationsJobs",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListLabelingJobsForWorkteam",
        "sagemaker:ListLineageGroups",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringExecutions",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
```

```
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListSubscribedWorkteams",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "sagemaker:PutLineageGroupPolicy",
        "sagemaker:PutModelPackageGroupPolicy",
        "sagemaker:PutRecord",
        "sagemaker:QueryLineage",
        "sagemaker:RegisterDevices",
        "sagemaker:RenderUiTemplate",
        "sagemaker:Search",
        "sagemaker:SendHeartbeat",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartHumanLoop",
        "sagemaker:StartMonitoringSchedule",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopEdgePackagingJob",
        "sagemaker:StopHumanLoop",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopInferenceRecommendationsJob",
        "sagemaker:StopLabelingJob",
        "sagemaker:StopMonitoringSchedule",
        "sagemaker:StopNotebookInstance",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateAction",
        "sagemaker:UpdateAppImageConfig",
        "sagemaker:UpdateArtifact",
```

```
        "sagemaker:UpdateCodeRepository",
        "sagemaker:UpdateContext",
        "sagemaker:UpdateDeviceFleet",
        "sagemaker:UpdateDevices",
        "sagemaker:UpdateDomain",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateExperiment",
        "sagemaker:UpdateImage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdateMonitoringSchedule",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:UpdateNotebookInstanceLifecycleConfig",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateProject",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:UpdateTrial",
        "sagemaker:UpdateTrialComponent",
        "sagemaker:UpdateUserProfile",
        "sagemaker:UpdateWorkforce",
        "sagemaker:UpdateWorkteam"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:action/*",
        "arn:aws:sagemaker:*:*:algorithm/*",
        "arn:aws:sagemaker:*:*:app-image-config/*",
        "arn:aws:sagemaker:*:*:artifact/*",
        "arn:aws:sagemaker:*:*:automl-job/*",
        "arn:aws:sagemaker:*:*:code-repository/*",
        "arn:aws:sagemaker:*:*:compilation-job/*",
        "arn:aws:sagemaker:*:*:context/*",
        "arn:aws:sagemaker:*:*:data-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:device-fleet/*/device/*",
        "arn:aws:sagemaker:*:*:device-fleet/*",
        "arn:aws:sagemaker:*:*:edge-packaging-job/*",
        "arn:aws:sagemaker:*:*:endpoint/*",
        "arn:aws:sagemaker:*:*:endpoint-config/*",
        "arn:aws:sagemaker:*:*:experiment/*",
        "arn:aws:sagemaker:*:*:experiment-trial/*",
        "arn:aws:sagemaker:*:*:experiment-trial-component/*",
        "arn:aws:sagemaker:*:*:feature-group/*",
        "arn:aws:sagemaker:*:*:human-loop/*",
        "arn:aws:sagemaker:*:*:human-task-ui/*",
```

```
        "arn:aws:sagemaker:*:*:hyper-parameter-tuning-job/*",
        "arn:aws:sagemaker:*:*:image/*",
        "arn:aws:sagemaker:*:*:image-version/*/*",
        "arn:aws:sagemaker:*:*:inference-recommendations-job/*",
        "arn:aws:sagemaker:*:*:labeling-job/*",
        "arn:aws:sagemaker:*:*:model/*",
        "arn:aws:sagemaker:*:*:model-bias-job-definition/*",
        "arn:aws:sagemaker:*:*:model-explainability-job-definition/*",
        "arn:aws:sagemaker:*:*:model-package/*",
        "arn:aws:sagemaker:*:*:model-package-group/*",
        "arn:aws:sagemaker:*:*:model-quality-job-definition/*",
        "arn:aws:sagemaker:*:*:monitoring-schedule/*",
        "arn:aws:sagemaker:*:*:notebook-instance/*",
        "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/*",
        "arn:aws:sagemaker:*:*:pipeline/*",
        "arn:aws:sagemaker:*:*:pipeline/*/execution/*",
        "arn:aws:sagemaker:*:*:processing-job/*",
        "arn:aws:sagemaker:*:*:project/*",
        "arn:aws:sagemaker:*:*:training-job/*",
        "arn:aws:sagemaker:*:*:transform-job/*",
        "arn:aws:sagemaker:*:*:workforce/*",
        "arn:aws:sagemaker:*:*:workteam/*"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AmazonSageMakerServiceCatalogProductsExecutionRole"
      ]
    },
    {
      "Sid" : "AmazonSageMakerLambdaLogPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DeleteLogDelivery",
        "logs:DescribeLogGroups",
```

```
        "logs:DescribeLogStreams",
        "logs:DescribeResourcePolicies",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeSubscriptionFilters",
        "logs:GetLogDelivery",
        "logs:GetLogEvents",
        "logs:ListLogDeliveries",
        "logs:PutLogEvents",
        "logs:PutResourcePolicy",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Sid" : "AmazonSageMakerLambdaCodeBuildPermission",
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:BatchGetBuilds"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/sagemaker-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/sagemaker:project-name" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerSpacesControllerPolicy

Beschreibung: Gewährt Systems Manager Manager-Aktivierungs-, Sitzungsverwaltungs- und KMS-Schlüsselbetriebsberechtigungen, die für das SageMaker Spaces-Addon erforderlich sind, um sicheren Fernzugriff auf EKS SageMaker Spaces zu ermöglichen.

`AmazonSageMakerSpacesControllerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerSpacesControllerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. November 2025, 04:34 UTC
- Bearbeitete Zeit: 19. November 2025, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesControllerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOperatorToSSMCreateActivationForSpaces",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateActivation"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeActivations",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeActivations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeSessions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeleteActivation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteActivation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToAddTagsToActivation",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:iam::*:role/sagemaker-space-*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeManagedNodes",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOperatorToSSMDeregisterWorkspaceInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeregisterManagedInstance"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToPassSsmManagedNodeRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/sagemaker-space-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowOperatorToSSMStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "ssm:resourceTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowStartSessionDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-StartSSHSession",
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToSSMDescribeDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/SageMaker-Space*"
      ]
    },
    {
      "Sid" : "AllowOperatorToSSMCreateDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces",
          "aws:RequestTag/sagemaker.amazonaws.com/eks-cluster-arn" :
 "${aws:PrincipalTag/eks-cluster-arn}"
        }
      }
    },
    {
      "Sid" : "AllowOperatorToEnableAdvancedTierForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting",
        "ssm:ResetServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/activation-
tier"
    },
    {
```

```
      "Sid" : "AllowOperatorToAddTagsToSSMDocument",
      "Effect" : "Allow",
      "Action" : "ssm:AddTagsToResource",
      "Resource" : "arn:aws:ssm:*:*:document/SageMaker-Space*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/sagemaker.amazonaws.com/managed-by" : "amazon-sagemaker-
spaces"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerSpacesRouterPolicy

Beschreibung: Erteilt Systems KMS-Schlüsselbetriebsberechtigungen, die für den SageMaker Spaces Router erforderlich sind, um einen sicheren Fernzugriff auf EKS SageMaker Spaces zu ermöglichen.

`AmazonSageMakerSpacesRouterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerSpacesRouterPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. November 2025, 04:34 UTC

- Bearbeitete Zeit: 19. November 2025, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerSpacesRouterPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "KMSKeyOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:sagemaker:component" : "amazon-sagemaker-spaces",
          "kms:EncryptionContext:sagemaker:eks-cluster-arn" : "${aws:PrincipalTag/eks-
cluster-arn}"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSageMakerTrainingPlanCreateAccess

Beschreibung: Diese von Amazon verwaltete Richtlinie bietet die erforderlichen Berechtigungen zum Erstellen und Verwalten von SageMaker Schulungsplänen. Sie ermöglicht es Benutzern, Schulungspläne und reservierte Kapazitäten zu erstellen, bestehende Schulungspläne zu beschreiben und Such- und Auflistungsvorgänge durchzuführen.

`AmazonSageMakerTrainingPlanCreateAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSageMakerTrainingPlanCreateAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2024, 13:21 UTC
- Zeit bearbeitet: 8. August 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSageMakerTrainingPlanCreateAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingPlan",
        "sagemaker:CreateReservedCapacity",
        "sagemaker:DescribeReservedCapacity"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Sid" : "AddTagsToTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "sagemaker:TaggingAction" : [
            "CreateTrainingPlan",
            "CreateReservedCapacity"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DescribeTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeTrainingPlan",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*"
      ]
    },
    {
      "Sid" : "NonResourceLevelTrainingPlanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:SearchTrainingPlanOfferings",
        "sagemaker:ListTrainingPlans"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListUltraServersByReservedCapacityPermissions",
      "Effect" : "Allow",
      "Action" : "sagemaker:ListUltraServersByReservedCapacity",
      "Resource" : [
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakeAdministrator

Beschreibung: Bietet vollen Zugriff auf Amazon Security Lake und zugehörige Services, die für die Verwaltung von Security Lake erforderlich sind.

`AmazonSecurityLakeAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSecurityLakeAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2023, 22:04 UTC
- Bearbeitete Zeit: 23. Februar 2024, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakeAdministrator`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsWithAnyResource",
      "Effect" : "Allow",
      "Action" : [
        "securitylake:*",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListAccounts",
        "iam:ListRoles",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowActionsWithAnyResourceViaSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCrawler",
        "glue:StopCrawlerSchedule",
        "lambda:CreateEventSourceMapping",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:GetDatalakeSettings",
        "events:ListConnections",
        "events:ListApiDestinations",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagingSecurityLakeS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaCreateFunction",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowLambdaAddPermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringEquals" : {
          "lambda:Principal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue:GetTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule",
        "events:CreateApiDestination",
        "events:CreateConnection",
        "events:UpdateConnection",
        "events:UpdateApiDestination",
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowSQSActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsCmkGrantForSecurityLake",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "GenerateDataKey",
            "RetireGrant",
            "Decrypt"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AllowEnablingQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:ResourceArn" : [
            "arn:aws:glue:*:*:catalog",
            "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
            "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringQueryBasedSubscribers",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:GetResourceShares",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : "LakeFormation*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowConfiguringCredentialsForSubscriberNotification",
      "Effect" : "Allow",
      "Action" : [
```

```
        "secretsmanager:CreateSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
```

```
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeS3ReplicationRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "s3.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:s3:::aws-security-data-lake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
      "Effect" : "Allow",
```

```
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForCustomSourceCrawlerGlueArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "glue.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationSecLakeArn",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:securitylake:*:*:subscriber/*"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleForSubscriberNotificationEventsArn",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "events.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceARN" : "arn:aws:events:*:*:rule/AmazonSecurityLake*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowOnboardingToSecurityLakeDependencies",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
        "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
        "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "securitylake.amazonaws.com",
            "lakeformation.amazonaws.com",
            "apidestinations.events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowRolePolicyActionsforSubscibersandSources",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:PutRolePolicy",
```

```
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowRegisterS3LocationInLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PutRolePolicy",
        "iam:GetRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowIAMActionsByResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRolePolicies",
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSecurityLake*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakes",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource" : "arn:aws:s3:::aws-security-data-lake-*"
    },
    {
      "Sid" : "S3ReadAccessToSecurityLakeMetastoreObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::security-lake-meta-store-manager-*"
    },
    {
      "Sid" : "S3ResourcelessReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakeMetastoreManager

Beschreibung: Richtlinie für Amazon SecurityLake Meta Store Manager Lambda, die den Zugriff auf Cloudwatch, S3, Glue und SQS ermöglicht.

`AmazonSecurityLakeMetastoreManager`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonSecurityLakeMetastoreManager` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 23. Januar 2024, 15:26 UTC
- Bearbeitete Zeit: 1. April 2024, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowWriteLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGlueManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowToReadFromSqs",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataReadWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCleanup",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSecurityLakePermissionsBoundary

Beschreibung: Amazon Security Lake erstellt IAM-Rollen für benutzerdefinierte Quellen von Drittanbietern, um Daten in einen Data Lake zu schreiben, und für Drittanbieter-Abonnenten, um Daten aus einem Data Lake zu nutzen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenze ihrer Berechtigungen zu definieren.

`AmazonSecurityLakePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSecurityLakePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2022, 14:11 UTC
- Bearbeitete Zeit: 14. Mai 2024, 20:39 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSecurityLakePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowActionsForSecurityLake",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsForSecurityLake",
      "Effect" : "Deny",
      "NotAction" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
```

```
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeBucket",
      "Effect" : "Deny",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeSQS",
      "Effect" : "Deny",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "NotResource" : "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid" : "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect" : "Deny",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:sqs:arn" : "false"
        },
        "StringNotLikeIfExists" : {
          "kms:EncryptionContext:aws:sqs:arn" : [
```

```
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SES über die AWS-Managementkonsole.

`AmazonSESFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSESFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SES über die AWS-Managementkonsole.

`AmazonSESReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSESReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 14. Mai 2024, 12:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSESReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SESReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ses:Get*",
        "ses:List*",
        "ses:BatchGetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSESServiceRolePolicy

Beschreibung: Ermöglicht SES, CloudWatch grundlegende Überwachungsmetriken von Amazon im Namen Ihrer SES-Ressourcen zu veröffentlichen

`AmazonSESServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Mai 2024, 16:02 UTC
- Bearbeitungszeit: 21. Mai 2024, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSESServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowPutMetricDataToSESCloudWatchNamespaces",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "AWS/SES",
            "AWS/SES/MailManager",
            "AWS/SES/Addons"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SNS über die AWS-Managementkonsole.

`AmazonSNSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSNSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. September 2024, 22:32 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSNSFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSFullAccess",
      "Effect" : "Allow",
      "Action" : "sns:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:CreateVerifiedDestinationNumber",
        "sms-voice:SendDestinationNumberVerificationCode",
        "sms-voice:SendTextMessage",
        "sms-voice:DeleteVerifiedDestinationNumber",
        "sms-voice:VerifyDestinationNumber",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:SetTextMessageSpendLimitOverride",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DeleteOptedOutNumber"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SNS über die AWS-Managementkonsole.

`AmazonSNSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSNSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. September 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSNSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SNSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:List*",
        "sns:CheckIfPhoneNumberIsOptedOut",
        "sns:GetEndpointAttributes",
        "sns:GetDataProtectionPolicy",
        "sns:GetPlatformApplicationAttributes",
        "sns:GetSMSAttributes",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMSAccessViaSNS",
      "Effect" : "Allow",
      "Action" : [
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribeOptedOutNumbers"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sns.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSNSRole

Beschreibung: Standardrichtlinie für die Amazon SNS SNS-Servicerolle.

`AmazonSNSRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSNSRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSNSRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSQSFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SQS über die AWS-Managementkonsole.

`AmazonSQSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSQSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sqs:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSQSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SQS über die AWS-Managementkonsole.

`AmazonSQSReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSQSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 24. Mai 2024, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSQSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonSQSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
```

```
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMAutomationApproverAccess

Beschreibung: Bietet Zugriff auf die Anzeige von Automatisierungsausführungen und das Senden von Genehmigungsentscheidungen an die Automatisierung, die auf ihre Genehmigung wartet

`AmazonSSMAutomationApproverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMAutomationApproverAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. August 2017, 23:07 UTC
- Bearbeitete Zeit: 7. August 2017, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMAutomationApproverAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution",
        "ssm:SendAutomationSignal"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMAutomationRole

Beschreibung: Stellt dem EC2 Automationsdienst Berechtigungen zur Ausführung von Aktivitäten bereit, die in Automatisierungsdokumenten definiert sind

`AmazonSSMAutomationRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMAutomationRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Dezember 2016, 22:09 UTC
- Bearbeitete Zeit: 11. September 2025, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMAutomationRole`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:Automation*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DeleteSnapshot",
        "ec2:StartInstances",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:Automation*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:*:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMDirectoryServiceAccess

Beschreibung: Diese Richtlinie ermöglicht es dem SSM-Agenten, im Namen des Kunden auf den Directory Service zuzugreifen, um der verwalteten Instanz einen Domänenbeitritt zu ermöglichen.

`AmazonSSMDirectoryServiceAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonSSMDirectoryServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2019, 17:44 Uhr UTC
- Bearbeitete Zeit: 15. März 2019, 17:44 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:CreateComputer",
        "ds:DescribeDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon SSM.

`AmazonSSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Mai 2015, 17:39 Uhr UTC
- Bearbeitete Zeit: 20. November 2019, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeInstanceStatus",
        "logs:*",
        "ssm:*",
        "ec2messages:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMMaintenanceWindowRole

Beschreibung: Servicerolle, die für das EC2 Wartungsfenster verwendet werden soll

`AmazonSSMMaintenanceWindowRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMMaintenanceWindowRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2016, 15:57 Uhr UTC
- Bearbeitete Zeit: 27. Juli 2019, 00:16 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonSSMMaintenanceWindowRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMManagedEC2InstanceDefaultPolicy

Beschreibung: Diese Richtlinie aktiviert die AWS Systems Manager Manager-Funktionalität auf EC2 Instanzen.

`AmazonSSMManagedEC2InstanceDefaultPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMManagedEC2InstanceDefaultPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. August 2022, 20:54 UTC
- Bearbeitete Zeit: 16. Juli 2024, 18:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMAgentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMChannelMessaging",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSSMLegacyMessaging",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMManagedInstanceCore

Beschreibung: Die Richtlinie für Amazon EC2 Role zur Aktivierung der Kernfunktionen des AWS Systems Manager Manager-Service.

`AmazonSSMManagedInstanceCore`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMManagedInstanceCore` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2019, 17:22 Uhr UTC
- Bearbeitete Zeit: 23. Mai 2019, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociation",
        "ssm:GetDeployablePatchSnapshotForInstance",
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:GetManifest",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:ListAssociations",
        "ssm:ListInstanceAssociations",
        "ssm:PutInventory",
        "ssm:PutComplianceItems",
        "ssm:PutConfigurePackageResult",
        "ssm:UpdateAssociationStatus",
        "ssm:UpdateInstanceAssociationStatus",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMPatchAssociation

Beschreibung: Ermöglichen Sie den Zugriff auf untergeordnete Instanzen für die Patchzuweisung.

`AmazonSSMPatchAssociation`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMPatchAssociation` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 13. Mai 2020, 16:00 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2020, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMPatchAssociation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribeEffectivePatchesForPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetPatchBaseline",
      "Resource" : "arn:aws:ssm:*:*:patchbaseline/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:DescribePatchBaselines",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon SSM.

`AmazonSSMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSSMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Mai 2015, 17:44 Uhr UTC
- Bearbeitete Zeit: 29. Mai 2015, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSSMServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von Amazon SSM verwaltet oder verwendet werden

`AmazonSSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2017, 19:20 Uhr UTC

- Bearbeitete Zeit: 15. Juli 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonSSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v16 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:GetAutomationExecution",
        "ssm:GetParameters",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListTagsForResource",
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutInventory"
      ],
```

```
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "ssm:InventoryTypeName" : [
            "AWS:ComplianceItem",
            "AWS:PatchSummary"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SSM*",
        "arn:aws:lambda:*:*:function:*:SSM*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "states:DescribeExecution",
        "states:StartExecution"
      ],
      "Resource" : [
        "arn:aws:states:*:*:stateMachine:SSM*",
        "arn:aws:states:*:*:execution:SSM*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:SelectResourceConfig"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEnrollmentStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeCases"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeComplianceByResource",
        "config:DescribeRemediationConfigurations",
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:ListStackSets",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStackInstances",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DeleteStackInstances",
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:PutRule",
        "events:PutTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/SSMExplorerManagedRule"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "events:DescribeRule",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "securityhub:DescribeHub",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-explorer-2:CreateManagedView",
      "Resource" : "arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonSumerianFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Sumerian.

`AmazonSumerianFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonSumerianFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. April 2018, 20:14 UTC
- Bearbeitete Zeit: 24. April 2018, 20:14 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonSumerianFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sumerian:*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTextractFullAccess

Beschreibung: Zugriff auf alle Amazon Textract APIs

`AmazonTextractFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTextractFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 19:07 UTC
- Bearbeitete Zeit: 28. November 2018, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTextractFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "textract:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTextractServiceRole

Beschreibung: Ermöglicht Textract, AWS Dienste in Ihrem Namen anzurufen.

`AmazonTextractServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTextractServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 28. November 2018, 19:12 Uhr UTC
- Zeit bearbeitet: 28. November 2018, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmazonTextractServiceRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:AmazonTextract*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Timestream mithilfe der AWS-Managementkonsole. Beachten Sie, dass diese Richtlinie auch Berechtigungen für bestimmte KMS-Operationen und Operationen zur Verwaltung Ihrer gespeicherten Abfragen gewährt. Wenn Sie vom Kunden verwaltetes CMK verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTimestreamConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 Uhr UTC
- Bearbeitete Zeit: 16. Oktober 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dbqms:CreateFavoriteQuery",
        "dbqms:DescribeFavoriteQueries",
        "dbqms:UpdateFavoriteQuery",
        "dbqms:DeleteFavoriteQueries",
        "dbqms:GetQueryString",
```

```
        "dbqms:CreateQueryHistory",
        "dbqms:DescribeQueryHistory",
        "dbqms:UpdateQueryHistory",
        "dbqms:DeleteQueryHistory"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
```

```
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:ListEntitlementDetails",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:Subscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-5jijo74ujy36m",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Timestream. Beachten Sie, dass diese Richtlinie auch Zugriff auf bestimmte KMS-Operationen gewährt. Wenn Sie vom Kunden verwaltetes CMK verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTimestreamFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 26. November 2021, 23:42 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:timestream:database-name"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "timestream.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBFullAccess

Beschreibung: Bietet vollen Administratorzugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon Timestream InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

`AmazonTimestreamInfluxDBFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTimestreamInfluxDBFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. März 2024, 22:53 UTC
- Bearbeitete Zeit: 16. Dezember 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
```

```
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "Resource" : "arn:aws:timestream-influxdb:*:*:*"
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid" : "MPViewAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MPSubscriptionAccessStatement",
      "Effect" : "Allow",
      "Action" : "aws-marketplace:Subscribe",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "prod-xcc5llpq4vlbc",
            "prod-rjppt7huo35fm"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess

Beschreibung: Bietet Administratorzugriff zur Verwaltung von Amazon Timestream InfluxDB-Instances und Parametergruppen mit Ausnahme von Marketplace-Vorgängen.

`AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. April 2025, 17:52 UTC
- Bearbeitete Zeit: 16. Dezember 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamInfluxDBFullAccessWithoutMarketplaceAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TimestreamInfluxDBStatement",
      "Effect" : "Allow",
      "Action" : [
        "timestream-influxdb:CreateDbParameterGroup",
        "timestream-influxdb:GetDbParameterGroup",
        "timestream-influxdb:ListDbParameterGroups",
        "timestream-influxdb:CreateDbInstance",
        "timestream-influxdb:DeleteDbInstance",
        "timestream-influxdb:GetDbInstance",
        "timestream-influxdb:ListDbInstances",
        "timestream-influxdb:TagResource",
        "timestream-influxdb:UntagResource",
        "timestream-influxdb:ListTagsForResource",
        "timestream-influxdb:UpdateDbInstance",
        "timestream-influxdb:CreateDbCluster",
        "timestream-influxdb:GetDbCluster",
        "timestream-influxdb:UpdateDbCluster",
        "timestream-influxdb:DeleteDbCluster",
        "timestream-influxdb:ListDbClusters",
        "timestream-influxdb:ListDbInstancesForCluster",
        "timestream-influxdb:RebootDbInstance",
        "timestream-influxdb:RebootDbCluster"
      ],
      "Resource" : [
        "arn:aws:timestream-influxdb:*:*:*"
      ]
    },
    {
      "Sid" : "ServiceLinkedRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/timestream-
influxdb.amazonaws.com/AWSServiceRoleForTimestreamInfluxDB",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "timestream-influxdb.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BucketValidationStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
```

```
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamInfluxDBServiceRolePolicy

Beschreibung: Bietet vollen Administratorzugriff zum Erstellen, Aktualisieren, Löschen und Auflisten von Amazon Timestream InfluxDB-Instances sowie zum Erstellen und Auflisten von Parametergruppen. Weitere erforderliche Berechtigungen finden Sie in der Dokumentation.

`AmazonTimestreamInfluxDBServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. März 2024, 18:53 UTC
- Bearbeitete Zeit: 14. März 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonTimestreamInfluxDBServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEniInSubnetStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "CreateEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "CreateTagWithEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonTimestreamInfluxDBManaged" : "false"
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEniStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonTimestreamInfluxDBManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PutCloudWatchMetricsStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Timestream/InfluxDB",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManageSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:READONLY-InfluxDB-auth-parameters-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTimestreamReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Timestream. Die Richtlinie gewährt auch die Erlaubnis, alle laufenden Abfragen abzubrechen. Wenn Sie vom Kunden verwaltetes CMK

verwenden, finden Sie in der Dokumentation nach, welche zusätzlichen Berechtigungen erforderlich sind.

`AmazonTimestreamReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTimestreamReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 21:47 UTC
- Bearbeitete Zeit: 5. Juni 2024, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTimestreamReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonTimestreamReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:CancelQuery",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
```

```
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:Select",
        "timestream:SelectValues",
        "timestream:DescribeScheduledQuery",
        "timestream:ListScheduledQueries",
        "timestream:DescribeBatchLoadTask",
        "timestream:ListBatchLoadTasks",
        "timestream:DescribeAccountSettings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTranscribeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Transcribe Transcribe-Operationen

`AmazonTranscribeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTranscribeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 16:06 UTC
- Bearbeitete Zeit: 4. April 2018, 16:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*transcribe*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonTranscribeReadOnlyAccess

Beschreibung: Bietet Zugriff auf den schreibgeschützten Betrieb für Amazon Transcribe

`AmazonTranscribeReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonTranscribeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 16:05 UTC
- Bearbeitete Zeit: 4. April 2018, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonTranscribeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transcribe:Get*",
        "transcribe:List*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVerifiedPermissionsFullAccess

Beschreibung: Bietet vollen Zugriff auf verifizierte Berechtigungen

`AmazonVerifiedPermissionsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVerifiedPermissionsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Oktober 2024, 18:19 UTC
- Bearbeitete Zeit: 11. Oktober 2024, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:CreatePolicyStore",
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:*"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVerifiedPermissionsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Dienst Verified Permissions.

`AmazonVerifiedPermissionsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVerifiedPermissionsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Oktober 2024, 18:25 UTC
- Bearbeitete Zeit: 11. Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVerifiedPermissionsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AccountLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:ListPolicyStores"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PolicyStoreLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
```

```
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyTemplates"
      ],
      "Resource" : [
        "arn:aws:verifiedpermissions::*:policy-store/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCCrossAccountNetworkInterfaceOperations

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Netzwerkschnittstellen und deren Verknüpfung mit kontoübergreifenden Ressourcen

`AmazonVPCCrossAccountNetworkInterfaceOperations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCCrossAccountNetworkInterfaceOperations` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 18. Juli 2017, 20:47 UTC
- Bearbeitete Zeit: 25. September 2023, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:ReplaceRoute"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfacePermissions",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon VPC über die AWS-Managementkonsole.

`AmazonVPCFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 9. Dezember 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
```

```
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpcPeeringConnection",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
```

```
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
```

```
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLink",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLink",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
```

```
        "ec2:ModifyVpcTenancy",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:RejectVpcPeeringConnection",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCNetworkAccessAnalyzerFullAccessPolicy

Beschreibung: Bietet Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Network Access Analyzer und zum Erstellen oder Löschen von Tags für Network Insights Access Scope und Network Insights Access Scope Analysis.

`AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCNetworkAccessAnalyzerFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Juni 2023, 22:56 UTC
- Bearbeitete Zeit: 15. Mai 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCNetworkAccessAnalyzerFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScope",
        "ec2:DeleteNetworkInsightsAccessScopeAnalysis",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAccessScopeAnalysis"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-access-scope/*",
        "arn:*:ec2:*:*:network-insights-access-scope-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:GetQueryAnswer"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerFullAccessPolicy

Beschreibung: Bietet Berechtigungen zum Beschreiben von AWS Ressourcen, zum Ausführen von Reachability Analyzer und zum Erstellen oder Löschen von Tags auf Network Insights Path und Network Insights Analysis.

`AmazonVPCReachabilityAnalyzerFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCReachabilityAnalyzerFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Juni 2023, 20:12 UTC
- Bearbeitete Zeit: 15. Mai 2024, 20:47 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "DirectconnectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
```

```
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-insights-path/*",
        "arn:*:ec2:*:*:network-insights-analysis/*"
      ]
    },
    {
      "Sid" : "ElasticloadbalancingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlobalacceleratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCustomRoutingAccelerators",
```

```
        "globalaccelerator:ListCustomRoutingEndpointGroups",
        "globalaccelerator:ListCustomRoutingListeners",
        "globalaccelerator:ListCustomRoutingPortMappings",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TirosPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

Beschreibung: Diese Richtlinie ist der Rolle zugeordnet IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess. Diese Rolle wird für die Mitgliedskonten in einer Organisation bereitgestellt, wenn das Verwaltungskonto den vertrauenswürdigen Zugriff für Reachability Analyzer ermöglicht. Es bietet Berechtigungen zum Anzeigen von Ressourcen aus Ihrer gesamten Organisation mithilfe der Reachability Analyzer-Konsole.

`AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCReachabilityAnalyzerPathComponentReadPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Mai 2023, 20:38 UTC
- Bearbeitete Zeit: 1. Mai 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewallPermissions",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:Describe*",
        "network-firewall:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonVPCReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon VPC über die AWS-Managementkonsole.

`AmazonVPCReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonVPCReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 9. Dezember 2024, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonVPCReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonVPCReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkDocsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon WorkDocs über AWS-Managementkonsole

`AmazonWorkDocsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkDocsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2020, 23:05 UTC
- Bearbeitete Zeit: 16. April 2020, 23:05 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkDocsReadOnlyAccess

Beschreibung: Bietet Nur-Lese-Zugriff auf Amazon WorkDocs über die AWS-Managementkonsole

`AmazonWorkDocsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkDocsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Januar 2020, 23:49 UTC
- Bearbeitete Zeit: 8. Januar 2020, 23:49 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkDocsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workdocs:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailEventsServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon WorkMail Events verwendet oder verwaltet werden

`AmazonWorkMailEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 16. April 2019, 16:52 UTC
- Bearbeitete Zeit: 16. April 2019, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkMailEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailFullAccess

Beschreibung: Bietet vollen Zugriff WorkMail auf Directory Service, SES EC2 und Lesezugriff auf KMS-Metadaten.

`AmazonWorkMailFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkMailFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 21. Dezember 2020, 14:13 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
```

```
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "events.workmail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.workmail.amazonaws.com/
AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*workmail*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "events.workmail.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailMessageFlowFullAccess

Beschreibung: Voller Zugriff auf den WorkMail Nachrichtenfluss APIs

`AmazonWorkMailMessageFlowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkMailMessageFlowFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2021, 11:08 UTC
- Bearbeitete Zeit: 11. Februar 2021, 11:08 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workmailmessageflow:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailMessageFlowReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf WorkMail Nachrichten für die GetRawMessageContent API

`AmazonWorkMailMessageFlowReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkMailMessageFlowReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Januar 2021, 12:40 Uhr UTC
- Bearbeitete Zeit: 28. Januar 2021, 12:40 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailMessageFlowReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workmailmessageflow:Get*"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkMailReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf WorkMail und SES.

`AmazonWorkMailReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkMailReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 25. Juli 2019, 08:24 UTC

- ARN: `arn:aws:iam::aws:policy/AmazonWorkMailReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesAdmin

Beschreibung: Bietet Zugriff auf WorkSpaces Amazon-Verwaltungsaktionen über AWS SDK und CLI.

`AmazonWorkSpacesAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesAdmin` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. September 2015, 22:21 Uhr UTC
- Bearbeitete Zeit: 27. Juni 2024, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesAdmin`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonWorkSpacesAdmin",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:ListAliases",
        "kms:ListKeys",
        "workspaces:CreateTags",
        "workspaces:CreateWorkspaceImage",
        "workspaces:CreateWorkspaces",
        "workspaces:CreateWorkspacesPool",
        "workspaces:CreateStandbyWorkspaces",
        "workspaces:DeleteTags",
        "workspaces:DeregisterWorkspaceDirectory",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaceBundles",
        "workspaces:DescribeWorkspaceDirectories",
        "workspaces:DescribeWorkspaces",
        "workspaces:DescribeWorkspacesPools",
        "workspaces:DescribeWorkspacesPoolSessions",
        "workspaces:DescribeWorkspacesConnectionStatus",
        "workspaces:ModifyCertificateBasedAuthProperties",
        "workspaces:ModifySamlProperties",
        "workspaces:ModifyStreamingProperties",
        "workspaces:ModifyWorkspaceCreationProperties",
        "workspaces:ModifyWorkspaceProperties",
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:RegisterWorkspaceDirectory",
        "workspaces:RestoreWorkspace",
        "workspaces:StartWorkspaces",
        "workspaces:StartWorkspacesPool",
        "workspaces:StopWorkspaces",
        "workspaces:StopWorkspacesPool",
        "workspaces:TerminateWorkspaces",
        "workspaces:TerminateWorkspacesPool",
        "workspaces:TerminateWorkspacesPoolSession",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesApplicationManagerAdminAccess

Beschreibung: Bietet Administratorzugriff für das Verpacken einer Anwendung in Amazon WorkSpaces Application Manager.

`AmazonWorkSpacesApplicationManagerAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesApplicationManagerAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. April 2015, 14:03 UTC
- Bearbeitete Zeit: 9. April 2015, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesApplicationManagerAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "wam:AuthenticatePackager",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkspacesPCAAccess

Beschreibung: Diese verwaltete Richtlinie bietet vollen Administratorzugriff auf AWS Certificate Manager Private CA-Ressourcen in Ihrem AWS-Konto für die zertifikatsbasierte Authentifizierung.

`AmazonWorkspacesPCAAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkspacesPCAAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. November 2022, 00:25 UTC
- Zeit bearbeitet: 8. November 2022, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:*:acm-pca:*:*:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/euc-private-ca" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesPoolServiceAccess

Beschreibung: Diese Richtlinie bietet AWS WorkSpaces Servicezugriff auf die erforderlichen Kundenkontoressourcen für den Start von Workspaces Pools

`AmazonWorkSpacesPoolServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesPoolServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2024, 16:21 UTC
- Bearbeitete Zeit: 27. Juni 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesPoolServiceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProvisioningWorkSpacesPoolPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "WorkSpacesPoolS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::wspool-logs-*",
        "arn:aws:s3:::wspool-app-settings-*",
        "arn:aws:s3:::wspool-home-folder-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesSecureBrowserReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon WorkSpaces Secure Browser und seine Abhängigkeiten über das SDK und die AWS-Managementkonsole CLI.

`AmazonWorkSpacesSecureBrowserReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesSecureBrowserReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2024, 20:01 UTC
- Bearbeitete Zeit: 24. Juni 2024, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSecureBrowserReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesSecureBrowser",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
```

```
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetIpAccessSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListIpAccessSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Sid" : "Dependencies",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesSelfServiceAccess

Beschreibung: Bietet Zugriff auf den WorkSpaces Amazon-Backend-Service zur Durchführung von Workspace Self Service-Aktionen

`AmazonWorkSpacesSelfServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesSelfServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 19:22 UTC
- Bearbeitete Zeit: 27. Juni 2019, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesSelfServiceAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "workspaces:RebootWorkspaces",
        "workspaces:RebuildWorkspaces",
        "workspaces:ModifyWorkspaceProperties"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesServiceAccess

Beschreibung: Ermöglicht Kundenkontozugriff auf den AWS WorkSpaces Service zum Starten eines Workspace.

`AmazonWorkSpacesServiceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesServiceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 19:19 UTC
- Bearbeitete Zeit: 18. März 2020, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesServiceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesThinClientFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon WorkSpaces Thin Client sowie eingeschränkten Zugriff auf erforderliche zugehörige Dienste

`AmazonWorkSpacesThinClientFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesThinClientFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. August 2024, 07:25 UTC
- Bearbeitete Zeit: 26. August 2025, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
monitoring.thinclient.amazonaws.com/
AWSServiceRoleForAmazonWorkSpacesThinClientMonitoring",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "monitoring.thinclient.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesThinClientMonitoringServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon WorkSpaces Thin Client Monitoring verwendet oder verwaltet werden

`AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Juni 2025, 19:37 UTC
- Bearbeitete Zeit: 13. Juni 2025, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesThinClientMonitoringServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesThinClient",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesThinClientReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon WorkSpaces Thin Client und seine Abhängigkeiten

`AmazonWorkSpacesThinClientReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesThinClientReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juli 2024, 08:50 UTC

- Zeit bearbeitet: 9. Januar 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesThinClientReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowThinClientReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowWorkSpacesAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowWorkSpacesSecureBrowserAccess",
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAppStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "appstream:DescribeStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesWebReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon WorkSpaces Web und seine Abhängigkeiten über das SDK und die AWS-Managementkonsole CLI.

`AmazonWorkSpacesWebReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonWorkSpacesWebReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2021, 14:20 Uhr UTC
- Zeit bearbeitet: 2. November 2022, 20:20 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonWorkSpacesWebReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
```

```
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
      ],
      "Resource" : "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonWorkSpacesWebServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon WorkSpaces Web verwendet oder verwaltet werden

`AmazonWorkSpacesWebServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2021, 13:15 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2022, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AmazonWorkSpacesWebServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "WorkSpacesWebManaged"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/WorkSpacesWebManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/WorkSpacesWeb",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStreamSummary"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonZocaloFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Zocalo.

`AmazonZocaloFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonZocaloFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:*",
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmazonZocaloReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Zocalo

`AmazonZocaloReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AmazonZocaloReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AmazonZocaloReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "zocalo:Describe*",
        "ds:DescribeDirectories",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AmplifyBackendDeployFullAccess

Beschreibung: Bietet Amplify-Vollzugriffsberechtigungen für die Bereitstellung von Amplify-Backend-Ressourcen (AWS AppSyncAmazon Cognito, Amazon S3 und andere verwandte Dienste) über das AWS Cloud Development Kit (CDK)AWS

`AmplifyBackendDeployFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AmplifyBackendDeployFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Oktober 2023, 21:32 UTC
- Bearbeitete Zeit: 14. November 2024, 19:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AmplifyBackendDeployFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CDKPreDeploy",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:GetTemplate",
```

```
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DeleteStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/amplify-*",
        "arn:aws:cloudformation:*:*:stack/CDKToolkit/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyMetadata",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "cloudformation:ListStacks",
        "ssm:DescribeParameters",
        "appsync:GetIntrospectionSchema",
        "amplify:GetBackendEnvironment"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AmplifyHotSwappableResources",
      "Effect" : "Allow",
      "Action" : [
        "appsync:GetSchemaCreationStatus",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:ListFunctions",
        "appsync:UpdateFunction",
        "appsync:UpdateApiKey"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AmplifyHotSwappableFunctionResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingListTags",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListTags"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:amplify-*"
      ]
    },
    {
      "Sid" : "AmplifySandboxLambdaLogsStreamingFilterLogEvents",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/amplify-*:*",
        "arn:aws:logs:*:*:log-group:amplify-*:*"
      ]
    },
    {
      "Sid" : "AmplifySchema",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::*amplify*",
        "arn:aws:s3:::cdk-*-assets-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CDKDeploy",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cdk-*-deploy-role-*-*",
        "arn:aws:iam::*:role/cdk-*-file-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-image-publishing-role-*-*",
        "arn:aws:iam::*:role/cdk-*-lookup-role-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath",
        "ssm:GetParameters",
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amplify/*",
        "arn:aws:ssm:*:*:parameter/cdk-bootstrap/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AmplifyModifySSMParam",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:DeleteParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/amplify/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmplifyDiscoverRDSVpcConfig",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBProxies",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "ec2:DescribeSubnets",
        "rds:DescribeDBSubnetGroups"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*",
        "arn:aws:rds:*:*:cluster:*",
        "arn:aws:rds:*:*:db-proxy:*",
        "arn:aws:rds:*:*:subgrp:*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

APIGatewayServiceRolePolicy

Beschreibung: Ermöglicht API Gateway, zugehörige AWS Ressourcen im Namen des Kunden zu verwalten.

`APIGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2017, 17:23 Uhr UTC
- Bearbeitete Zeit: 12. Juli 2021, 22:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/APIGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddListenerCertificates",
        "elasticloadbalancing:RemoveListenerCertificates",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/amazon-apigateway-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:GetCertificate"
      ],
```

```
      "Resource" : "arn:aws:acm:*:*:certificate/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Owner",
            "VpcLinkId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetNamespace",
      "Resource" : "arn:aws:servicediscovery:*:*:namespace/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "servicediscovery:GetService",
      "Resource" : "arn:aws:servicediscovery:*:*:service/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppIntegrationsServiceLinkedRolePolicy

Beschreibung: Ermöglicht AppIntegrations die Verwaltung von AppFlow Ressourcen und die Veröffentlichung von CloudWatch Metrikdaten in Ihrem Namen.

`AppIntegrationsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. September 2022, 19:42 UTC
- Bearbeitete Zeit: 30. September 2022, 19:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppIntegrationsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppIntegrations"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorEntity",
        "appflow:ListConnectorEntities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeConnectorProfiles",
        "appflow:UseConnectorProfile"
      ],
      "Resource" : "arn:aws:appflow:*:*:connector-profile/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AppIntegrationsManaged" : "true"
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:TagResource"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppIntegrationsManaged"
          ]
        }
      },
      "Resource" : "arn:aws:appflow:*:*:flow/FlowCreatedByAppIntegrations-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ApplicationAutoScalingForAmazonAppStreamAccess

Beschreibung: Richtlinie zur Aktivierung von Application Autoscaling für Amazon AppStream

`ApplicationAutoScalingForAmazonAppStreamAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ApplicationAutoScalingForAmazonAppStreamAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2017, 21:39 Uhr UTC
- Zeit bearbeitet: 6. Februar 2017, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ApplicationAutoScalingForAmazonAppStreamAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
```

```
        "appstream:DescribeFleets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von der Funktion Application Discovery Service Continuous Export verwendet oder verwaltet werden

`ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. August 2018, 20:22 UTC
- Bearbeitete Zeit: 13. August 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
```

```
        "firehose:UpdateDestination"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:firehose:*:*:deliverystream/aws-application-discovery-
service*"
    },
    {
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3:::aws-application-discovery-service*/*"
    },
    {
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose*"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    },
```

```
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "firehose.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppRunnerNetworkingServiceRolePolicy

Beschreibung: Ermöglicht AWS AppRunner Networking, verwandte AWS Ressourcen in Ihrem Namen zu verwalten.

`AppRunnerNetworkingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Januar 2022, 21:02 UTC

- Bearbeitete Zeit: 12. Januar 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerNetworkingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSAppRunnerManaged"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "StringLike" : {
          "aws:RequestTag/AWSAppRunnerManaged" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSAppRunnerManaged" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppRunnerServiceRolePolicy

Beschreibung: Ermöglicht AWS AppRunner die Verwaltung verwandter AWS Ressourcen in Ihrem Namen.

`AppRunnerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Mai 2021, 19:15 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppRunnerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/apprunner/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/apprunner/*:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSAppRunnerManagedRule*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AppStudioServiceRolePolicy

Beschreibung: Ermöglicht AppStudio die Verwaltung der zugehörigen AWS Ressourcen in Ihrem Namen.

`AppStudioServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juli 2024, 05:01 UTC
- Bearbeitete Zeit: 13. März 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AppStudioServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppStudioResourcePermissionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appstudio/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSecretsManager",
```

```
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "IsAppStudioSecret"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/IsAppStudioSecret" : "true"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForManagedSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appstudio"
        }
      }
    },
    {
      "Sid" : "AppStudioResourceWritePermissionsForManagedSecrets",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:appstudio!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AppStudioResourcePermissionsForSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AuroraDsqlServiceLinkedRolePolicy

Beschreibung: Richtlinie für Amazon Aurora DSQL Service Linked Role

`AuroraDsqlServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. Dezember 2024, 15:06 Uhr UTC
- Bearbeitete Zeit: 09. Mai 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AuroraDsqlServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/AuroraDSQL",
            "AWS/Usage"
```

```
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf Auto Scaling über die AWS-Managementkonsole.

`AutoScalingConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AutoScalingConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:43 UTC
- Bearbeitete Zeit: 6. Februar 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:ImportKeyPair"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:Describe*"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Auto Scaling über die. AWS-Managementkonsole

`AutoScalingConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AutoScalingConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:48 UTC
- Bearbeitete Zeit: 12. Januar 2017, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListSubscriptions",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingFullAccess

Beschreibung: Bietet vollen Zugriff auf Auto Scaling.

`AutoScalingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AutoScalingFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:31 UTC
- Bearbeitete Zeit: 6. Februar 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingNotificationAccessRole

Beschreibung: Standardrichtlinie für die Servicerolle AutoScaling Notification Access.

`AutoScalingNotificationAccessRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AutoScalingNotificationAccessRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AutoScalingNotificationAccessRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Auto Scaling.

`AutoScalingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AutoScalingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2017, 19:39 UTC
- Zeit bearbeitet: 12. Januar 2017, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AutoScalingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "autoscaling:Describe*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AutoScalingServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Auto Scaling verwendet oder verwaltet werden

`AutoScalingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Januar 2018, 23:10 Uhr UTC
- Zeit bearbeitet: 12. November 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AutoScalingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachClassicLinkVpc",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CreateReplaceRootVolumeTask",
        "ec2:CreateFleet",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
```

```
        "ec2:DetachClassicLinkVpc",
        "ec2:GetInstanceTypesFromInstanceRequirements",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyInstanceAttribute",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2InstanceProfileManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com*"
        }
      }
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ELBManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Register*",
        "elasticloadbalancing:Deregister*",
```

```
        "elasticloadbalancing:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWManagement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSManagement",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgeRuleManagement",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerParameterManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeManagement",
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:DeregisterTargets",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListTargets",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:RegisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceGroupsManagement",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-Automation-DiagnosisBucketPolicy

Beschreibung: Stellt Berechtigungen für den Zugriff auf den SSM Diagnosis S3-Bucket zur Diagnose und Behebung von Problemen bereit.

`AWS-SSM-Automation-DiagnosisBucketPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-Automation-DiagnosisBucketPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 23:31 UTC
- Bearbeitete Zeit: 15. November 2024, 23:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*/
${aws:PrincipalAccount}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowReadOnlyAccessListBucketOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
```

```
        },
        "StringLike" : {
          "s3:prefix" : "*/${aws:PrincipalAccount}/*"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowGetEncryptionConfigurationOnSsmDiagnosisBucketWithinOrg",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

Beschreibung: Erteilen Sie die Berechtigung zur Diagnose von Problemen mit SSM-Diensten, indem Sie Aktivitäten ausführen, die in Automatisierungsdokumenten definiert sind. Diese werden hauptsächlich für die Ausführung der Automatisierungsdokumente in einer kontoübergreifenden, regionsübergreifenden Konfiguration verwendet, indem untergeordnete Automatisierungen innerhalb von Mitgliedskonten ausgelöst werden.

`AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. November 2024, 00:01 UTC
- Bearbeitete Zeit: 16. Juli 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
```

```
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

Beschreibung: Erteilen Sie die Berechtigung zur Diagnose von Problemen mit SSM-Diensten, indem Sie Aktivitäten ausführen, die in Automatisierungsdokumenten definiert sind. Diese werden hauptsächlich für die Ausführung der Automatisierungsdokumente in einer account/region Zielkonfiguration verwendet, indem die Integrität des SSM-Dienstes auf allen Knoten diagnostiziert wird.

`AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. November 2024, 00:08 UTC

- Bearbeitete Zeit: 16. Juli 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationStepExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:GetAutomationExecution"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-*UnmanagedEC2*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-*UnmanagedEC2*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

Beschreibung: Stellt Betriebskonten Berechtigungen zur Diagnose nicht verwalteter Knoten bereit, indem organisationsspezifische Berechtigungen erteilt werden, die für die SSM-Automatisierung erforderlich sind, um die Liste der Mitgliedskonten innerhalb eines Stammverzeichnisses einer Organisation abzurufen und die kontenübergreifende Ausführung auszulösen, indem die Übernahme von Ausführungsrollen im Zielkonto/in der Zielregion ermöglicht wird.

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`ist eine verwaltete AWS Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 16. November 2024, 00:11 UTC
- Zeit bearbeitet: 16. November 2024, 00:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeDiagnosisExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-RemediationAutomation-AdministrationRolePolicy

Beschreibung: Erteilen Sie die Erlaubnis zur Behebung von Problemen mit SSM-Diensten durch Ausführung von Aktivitäten, die in Automatisierungsdokumenten definiert sind. Diese werden hauptsächlich für die Ausführung von Automatisierungsdokumenten in einer kontoübergreifenden, regionsübergreifenden Konfiguration verwendet, indem untergeordnete Automatisierungen innerhalb von Mitgliedskonten ausgelöst werden.

`AWS-SSM-RemediationAutomation-AdministrationRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-RemediationAutomation-AdministrationRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. November 2024, 00:14 UTC
- Bearbeitete Zeit: 16. Juli 2025, 17:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-AdministrationRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinAccount",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowReadWriteToSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*/actions/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListBucketOnSsmDiagnosisBucketInSameAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-diagnosis-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-RemediationAutomation-ExecutionRolePolicy

Beschreibung: Bietet Berechtigungen zur Behebung von Problemen mit SSM-Diensten durch Ausführung von Aktivitäten, die in Automatisierungsdokumenten definiert sind. Diese werden

hauptsächlich für die Ausführung der Automatisierungsdokumente in einer account/region Zielkonfiguration verwendet, indem die Integrität der SSM-Dienste auf allen Knoten wiederhergestellt wird.

`AWS-SSM-RemediationAutomation-ExecutionRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. November 2024, 00:17 UTC
- Bearbeitete Zeit: 16. Juli 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-ExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessSSMResource",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyAccessEC2Resource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateVpcEndpointForTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "RestrictCreateVpcEndpointForSSMService",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : [
            "com.amazonaws.*.ssm",
            "com.amazonaws.*.ssmmessages",
            "com.amazonaws.*.ec2messages"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint"
        }
      }
    },
    {
      "Sid" : "RestrictCreateVpcEndpointWithTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingVPCEndpoints::VPCE" :
"VPCEndpoint",
          "ec2:CreateAction" : [
            "CreateVpcEndpoint"
          ]
        }
      }
    },
    {
      "Sid" : "AllowModifyVpcAttributeForDns",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Attribute" : [
            "EnableDnsSupport",
            "EnableDnsHostnames"
          ]
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateForTaggedResource",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess"
        }
      }
    },
    {
      "Sid" : "AllowSecurityGroupRuleUpdateTagRule",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::SG::Rule" :
"HTTPSAccess",
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupEgress",
            "AuthorizeSecurityGroupIngress"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateSecurityGroupForVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "AllowCreateSecurityGroupWithTag",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup"
        }
      }
    },
    {
      "Sid" : "AllowTagCreationForSecurityGroupTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManager::FindingNetworkingSecurityGroups::VPCE::SG" :
"VPCEndpointSecurityGroup",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "AllowExecuteSSMAutomation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-OrchestrateUnmanagedEC2Actions",
        "arn:aws:ssm:*:*:document/AWS-RemediateSSMAgent*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWS-OrchestrateUnmanagedEC2Actions:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RemediateSSMAgent*:*"
      ]
    },
    {
```

```
      "Sid" : "AllowKMSOperations",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleOnSelfToSsm",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

Beschreibung: Erlaubt Betriebskonten Berechtigungen zur Behebung nicht verwalteter Knoten, indem organisationsspezifische Berechtigungen bereitgestellt werden, die für die SSM-Automatisierung erforderlich sind, um die Liste der Mitgliedskonten innerhalb eines Stammverzeichnisses einer Organisation abzurufen und die kontenübergreifende Ausführung auszulösen, indem die Übernahme von Ausführungsrollen im Zielkonto/in der Zielregion ermöglicht wird.

`AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`ist eine verwaltete AWS Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. November 2024, 00:25 UTC
- Bearbeitete Zeit: 16. November 2024, 00:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyAccessOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeRemediationExecutionRoleWithinOrg",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgId" : "${aws:PrincipalOrgId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWS_ConfigRole

Beschreibung: Standardrichtlinie für die AWS Config-Dienstrolle. Stellt die für AWS Config erforderlichen Berechtigungen bereit, um Änderungen an Ihren AWS Ressourcen nachzuverfolgen.

`AWS_ConfigRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWS_ConfigRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. September 2020, 20:30 Uhr UTC
- Bearbeitete Zeit: 21. November 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWS_ConfigRole`

Version der Richtlinie

Richtlinienversion: v42 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigRoleStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
```

```
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
```

```
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
```

```
            "apprunner:DescribeVpcConnector",
            "apprunner:DescribeVpcIngressConnection",
            "apprunner:ListObservabilityConfigurations",
            "apprunner:ListServices",
            "apprunner:ListTagsForResource",
            "apprunner:ListVpcConnectors",
            "appstream:DescribeAppBlockBuilders",
            "appstream:DescribeApplications",
            "appstream:DescribeDirectoryConfigs",
            "appstream:DescribeFleets",
            "appstream:DescribeStacks",
            "appstream:ListTagsForResource",
            "appsync:GetApiCache",
            "appsync:GetGraphqlApi",
            "appsync:GetSourceApiAssociation",
            "appsync:ListGraphqlApis",
            "appsync:ListSourceApiAssociations",
            "aps:DescribeAlertManagerDefinition",
            "aps:DescribeLoggingConfiguration",
            "APS:DescribeRuleGroupsNamespace",
            "APS:DescribeWorkspace",
            "aps:ListRuleGroupsNamespaces",
            "aps:ListTagsForResource",
            "APS:ListWorkspaces",
            "application-signals:ListServiceLevelObjectiveExclusionWindows",
            "application-signals:ListTagsForResource",
            "apprunner:DescribeAutoScalingConfiguration",
            "apprunner:ListAutoScalingConfigurations",
            "apprunner:ListVpcIngressConnections",
            "appstream:DescribeAppBlocks",
            "appstream:DescribeImageBuilders",
            "appsync:GetApi",
            "appsync:GetDomainName",
            "appsync:ListApis",
            "appsync:ListDomainNames",
            "appsync:ListTagsForResource",
            "apptest:GetTestCase",
            "apptest:ListTagsForResource",
            "apptest:ListTestCases",
            "aps:DescribeScraper",
            "aps:DescribeScraperLoggingConfiguration",
            "aps:ListScrapers",
            "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
            "athena:GetDataCatalog",
```

```
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
```

```
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
```

```
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
```

```
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:GetDashboard",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
```

```
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
```

```
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
```

```
            "connect:DescribeView",
            "connect:GetTaskTemplate",
            "connect:ListApprovedOrigins",
            "connect:ListEvaluationForms",
            "connect:ListInstanceAttributes",
            "connect:ListInstances",
            "connect:ListInstanceStorageConfigs",
            "connect:ListIntegrationAssociations",
            "connect:ListPhoneNumbers",
            "connect:ListPhoneNumbersV2",
            "connect:ListPredefinedAttributes",
            "connect:ListPrompts",
            "connect:ListQueueQuickConnects",
            "connect:ListQueues",
            "connect:ListQuickConnects",
            "connect:ListRoutingProfileQueues",
            "connect:ListRoutingProfiles",
            "connect:ListRules",
            "connect:ListSecurityKeys",
            "connect:ListSecurityProfileApplications",
            "connect:ListSecurityProfilePermissions",
            "connect:ListSecurityProfiles",
            "connect:ListTagsForResource",
            "connect:ListTaskTemplates",
            "connect:ListTrafficDistributionGroups",
            "connect:ListUsers",
            "connect:ListViewVersions",
            "connect:ListViews",
            "connect:SearchAvailablePhoneNumbers",
            "databrew:DescribeDataset",
            "databrew:DescribeJob",
            "databrew:DescribeProject",
            "databrew:DescribeRecipe",
            "databrew:DescribeRuleset",
            "databrew:DescribeSchedule",
            "databrew:ListDatasets",
            "databrew:ListJobs",
            "databrew:ListProjects",
            "databrew:ListRecipes",
            "databrew:ListRecipeVersions",
            "databrew:ListRulesets",
            "databrew:ListSchedules",
            "datasync:DescribeAgent",
            "datasync:DescribeLocationEfs",
```

```
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetMonitor",
        "deadline:GetQueueFleetAssociation",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListMonitors",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListTagsForResource",
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
```

```
            "dms:DescribeDataMigrations",
            "dms:DescribeEndpoints",
            "dms:DescribeEventSubscriptions",
            "dms:DescribeReplicationConfigs",
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationSubnetGroups",
            "dms:DescribeReplicationTaskAssessmentRuns",
            "dms:DescribeReplicationTasks",
            "dms:ListMigrationProjects",
            "dms:ListTagsForResource",
            "ds:DescribeDirectories",
            "ds:DescribeDomainControllers",
            "ds:DescribeEventTopics",
            "ds:ListLogSubscriptions",
            "ds:ListTagsForResource",
            "dynamodb:DescribeContinuousBackups",
            "dynamodb:DescribeGlobalTable",
            "dynamodb:DescribeGlobalTableSettings",
            "dynamodb:DescribeLimits",
            "dynamodb:DescribeTable",
            "dynamodb:DescribeTableReplicaAutoScaling",
            "dynamodb:DescribeTimeToLive",
            "dynamodb:ListTables",
            "dynamodb:ListTagsOfResource",
            "ec2:Describe*",
            "ec2:GetAllowedImagesSettings",
            "ec2:GetEbsEncryptionByDefault",
            "ec2:GetInstanceTypesFromInstanceRequirements",
            "ec2:GetIpamPoolAllocations",
            "ec2:GetIpamPoolCidrs",
            "ec2:GetManagedPrefixListEntries",
            "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
            "ec2:GetNetworkInsightsAccessScopeContent",
            "ec2:GetSnapshotBlockPublicAccessState",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:GetVerifiedAccessGroupPolicy",
            "ec2:SearchLocalGatewayRoutes",
            "ec2:SearchTransitGatewayMulticastGroups",
            "ecr-public:DescribeRepositories",
            "ecr-public:GetRepositoryCatalogData",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:ListTagsForResource",
            "ecr:BatchGetRepositoryScanningConfiguration",
            "ecr:DescribePullThroughCacheRules",
```

```
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
```

```
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
```

```
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
```

```
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
```

```
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
```

```
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
```

```
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
```

```
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
```

```
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
```

```
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
```

```
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
```

```
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
```

```
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
```

```
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
```

```
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
```

```
            "managedblockchain:GetNetwork",
            "managedblockchain:GetNode",
            "managedblockchain:ListAccessors",
            "managedblockchain:ListInvitations",
            "managedblockchain:ListMembers",
            "managedblockchain:ListNodes",
            "mediaconnect:DescribeBridge",
            "mediaconnect:DescribeFlow",
            "mediaconnect:DescribeGateway",
            "mediaconnect:ListBridges",
            "mediaconnect:ListFlows",
            "mediaconnect:ListGateways",
            "mediaconnect:ListTagsForResource",
            "medialive:DescribeChannelPlacementGroup",
            "medialive:DescribeMultiplexProgram",
            "medialive:ListChannelPlacementGroups",
            "medialive:ListMultiplexPrograms",
            "medialive:ListMultiplexes",
            "medialive:ListTagsForResource",
            "mediapackage-vod:DescribeAsset",
            "mediapackage-vod:DescribePackagingConfiguration",
            "mediapackage-vod:DescribePackagingGroup",
            "mediapackage-vod:ListAssets",
            "mediapackage-vod:ListPackagingConfigurations",
            "mediapackage-vod:ListPackagingGroups",
            "mediapackage-vod:ListTagsForResource",
            "mediapackagev2:GetChannel",
            "mediapackagev2:GetChannelGroup",
            "mediapackagev2:GetOriginEndpoint",
            "mediapackagev2:ListChannelGroups",
            "mediapackagev2:ListChannels",
            "mediapackagev2:ListOriginEndpoints",
            "mediatailor:DescribeChannel",
            "mediatailor:DescribeLiveSource",
            "mediatailor:DescribeSourceLocation",
            "mediatailor:DescribeVodSource",
            "mediatailor:GetPlaybackConfiguration",
            "mediatailor:ListChannels",
            "mediatailor:ListLiveSources",
            "mediatailor:ListPlaybackConfigurations",
            "mediatailor:ListSourceLocations",
            "mediatailor:ListVodSources",
            "memorydb:DescribeAcls",
            "memorydb:DescribeClusters",
```

```
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
```

```
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
```

```
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
```

```
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
```

```
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
```

```
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
```

```
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
```

```
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAbac",
        "s3:GetBucketAcl",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
```

```
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
```

```
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTags",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkteams",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "sdb:GetAttributes",
```

```
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
        "securityhub:DescribeHub",
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serviceCatalog:DescribePortfolioShares",
        "servicecatalog:DescribeServiceAction",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListServiceActions",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicediscovery:GetInstance",
        "servicediscovery:GetNamespace",
        "servicediscovery:GetService",
        "servicediscovery:ListInstances",
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
```

```
        "ses:ListReceiptRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
        "ssm-contacts:ListContacts",
        "ssm-contacts:ListTagsForResource",
        "ssm-incidents:GetReplicationSet",
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:ListReplicationSets",
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:ListTagsForResource",
        "ssm-quicksetup:GetConfigurationManager",
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-sap:ListTagsForResource",
        "ssm:DescribeAssociation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeDocument",
        "ssm:DescribeDocumentPermission",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
```

```
        "ssm:DescribePatchBaselines",
        "ssm:GetAutomationExecution",
        "ssm:GetDefaultPatchBaseline",
        "ssm:GetDocument",
        "ssm:GetPatchBaseline",
        "ssm:GetResourcePolicies",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSet",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSets",
        "sso:ListTagsForResource",
        "states:DescribeActivity",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineAlias",
        "states:ListActivities",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:ListTagsForResource",
        "storagegateway:ListVolumes",
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
```

```
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
```

```
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigLogStreamStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "ConfigLogEventsStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountActivityAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf die Seite mit den Kontoaktivitäten.

`AWSAccountActivityAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAccountActivityAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 7. März 2023, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountActivityAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
```

```
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "payments:ListPaymentPreferences"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountManagementFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Kontoverwaltung.

`AWSAccountManagementFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAccountManagementFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 30. September 2021, 23:20 Uhr UTC
- Bearbeitete Zeit: 30. September 2021, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "account:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountManagementReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Kontoverwaltung AWS

`AWSAccountManagementReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAccountManagementReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2021, 23:29 Uhr UTC
- Bearbeitete Zeit: 30. September 2021, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountManagementReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:Get*",
        "account:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountSettingsManagementRole

Beschreibung: Stellt die erforderlichen Berechtigungen zur Verwaltung eines Benutzerkontos für AWS Anwendungen bereit.

`AWSAccountSettingsManagementRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAccountSettingsManagementRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2025, 17:49 UTC
- Bearbeitete Zeit: 11. Dezember 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountSettingsManagementRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:GetAccountInformation",
        "account:CloseAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "payments:ListTagsForResource",
        "payments:UntagResource",
        "payments:TagResource",
        "payments:ListPaymentPreferences",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:MakePayment",
        "payments:UpdatePaymentPreferences",
        "payments:CreatePaymentInstrument",
        "payments:UpdatePaymentInstrument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "invoicing:GetInvoicePDF"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetSellerOfRecord"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ce:GetCostAndUsage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tax:GetTaxRegistration",
        "tax:PutTaxRegistration",
        "tax:ListTaxRegistrations",
        "tax:DeleteTaxRegistration",
        "tax:BatchPutTaxRegistration",
        "tax:GetTaxRegistrationDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "customer-verification:CreateCustomerVerificationDetails",
        "customer-verification:CreateUploadUrls",
        "customer-verification:UpdateCustomerVerificationDetails"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:ListApplications"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAccountUsageReportAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf die Seite mit dem Kontonutzungsbericht.

`AWSAccountUsageReportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAccountUsageReportAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAccountUsageReportAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewUsage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAgentlessDiscoveryService

Beschreibung: Ermöglicht den Zugriff für den Discovery Agentless Connector zur Registrierung beim AWS Application Discovery Service.

`AWSAgentlessDiscoveryService`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAgentlessDiscoveryService` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. August 2016, 01:35 UTC
- Bearbeitete Zeit: 24. Februar 2020, 23:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAgentlessDiscoveryService`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "awsconnector:RegisterConnector",
        "awsconnector:GetConnectorHealth"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade/*",
        "arn:aws:s3:::prod.agentless.discovery.connector.upgrade"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-connector-debug-logs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    },
    {
      "Sid" : "Discovery",
      "Effect" : "Allow",
      "Action" : [
        "Discovery:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "arsenal",
      "Effect" : "Allow",
      "Action" : [
```

```
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS AppFabric Dienst und schreibgeschützten Zugriff auf abhängige Dienste wie S3, Kinesis, KMS.

`AWSAppFabricFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppFabricFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:51 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSListAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FirehoseReadAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUseOfServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appfabric.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS AppFabric

`AWSAppFabricReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppFabricReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 19:52 UTC
- Bearbeitete Zeit: 27. Juni 2023, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppFabricReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppFabricServiceRolePolicy

Beschreibung: Ermöglicht AppFabric den Zugriff auf AWS Ressourcen in Ihrem Namen

`AWSAppFabricServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2023, 21:07 UTC
- Bearbeitete Zeit: 26. Juni 2023, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppFabricServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEmitMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/AppFabric"
        }
      }
    },
    {
      "Sid" : "S3PutObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSAppFabric/*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FirehosePutRecord",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecordBatch"
      ],
      "Resource" : "arn:aws:firehose:*:*:deliverystream/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/AWSAppFabricManaged" : "true"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingAppStreamFleetPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt AppStream und CloudWatch.

`AWSApplicationAutoscalingAppStreamFleetPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2017, 19:04 Uhr UTC
- Bearbeitete Zeit: 20. Oktober 2017, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingAppStreamFleetPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appstream:UpdateFleet",
        "appstream:DescribeFleets",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingCassandraTablePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Cassandra gewährt und CloudWatch.

`AWSApplicationAutoscalingCassandraTablePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. März 2020, 22:49 UTC
- Bearbeitete Zeit: 18. März 2020, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingCassandraTablePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cassandra:Select",
      "Resource" : [
        "arn:*:cassandra:*:*:/keyspace/system/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema/table/*",
        "arn:*:cassandra:*:*:/keyspace/system_schema_mcs/table/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Alter",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingComprehendEndpointPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Comprehend und gewährt. CloudWatch

`AWSApplicationAutoscalingComprehendEndpointPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2019, 18:39 Uhr UTC
- Bearbeitete Zeit: 14. November 2019, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingComprehendEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:UpdateEndpoint",
        "comprehend:DescribeEndpoint",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoScalingCustomResourcePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen APIGateway und CloudWatch benutzerdefinierte Ressourcenskalierung gewährt

`AWSApplicationAutoScalingCustomResourcePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Juni 2018, 23:22 UTC
- Bearbeitete Zeit: 4. Juni 2018, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoScalingCustomResourcePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingDynamoDBTablePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf DynamoDB gewährt und. CloudWatch

`AWSApplicationAutoscalingDynamoDBTablePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2017, 21:34 UTC
- Zeit bearbeitet: 20. Oktober 2017, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingDynamoDBTablePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingEC2SpotFleetRequestPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf EC2 Spot Fleet gewährt und CloudWatch.

`AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2017, 18:23 Uhr UTC
- Zeit bearbeitet: 25. Oktober 2017, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEC2SpotFleetRequestPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingECSServicePolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf EC2 Container Service gewährt und CloudWatch.

`AWSApplicationAutoscalingECSServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2017, 23:53 Uhr UTC
- Bearbeitete Zeit: 24. Oktober 2024, 20:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingECSServicePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeServices",
        "ecs:UpdateService",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingElastiCacheRGPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon ElastiCache und Amazon gewährt CloudWatch.

`AWSApplicationAutoscalingElastiCacheRGPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. August 2021, 23:41 UTC
- Bearbeitete Zeit: 26. März 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingElastiCacheRGPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheActionsOnAllClusters",
      "Effect" : "Allow",
      "Action" : [
        "elasticache:DescribeReplicationGroups",
        "elasticache:ModifyCacheCluster",
        "elasticache:ModifyReplicationGroupShardConfiguration",
        "elasticache:IncreaseReplicaCount",
        "elasticache:DecreaseReplicaCount",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameters"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingEMRInstanceGroupPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen für Elastic Map Reduce gewährt und CloudWatch.

`AWSApplicationAutoscalingEMRInstanceGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Oktober 2017, 00:57 UTC
- Zeit bearbeitet: 26. Oktober 2017, 00:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingEMRInstanceGroupPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ModifyInstanceGroups",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingKafkaClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Managed Streaming for Apache Kafka gewährt und CloudWatch.

`AWSApplicationAutoscalingKafkaClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2020, 18:36 Uhr UTC
- Zeit bearbeitet: 24. August 2020, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingKafkaClusterPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:UpdateBrokerStorage",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingLambdaConcurrencyPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Lambda gewährt und CloudWatch.

`AWSApplicationAutoscalingLambdaConcurrencyPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Oktober 2019, 20:04 UTC
- Bearbeitete Zeit: 21. Oktober 2019, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingLambdaConcurrencyPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:DeleteProvisionedConcurrencyConfig",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingNeptuneClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon Neptune und Amazon gewährt. CloudWatch

`AWSApplicationAutoscalingNeptuneClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 02. September 2021, 21:14 UTC
- Bearbeitete Zeit: 02. September 2021, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingNeptuneClusterPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterParameters",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:AddTagsToResource",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "rds:CreateDBInstance",
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*",
        "arn:aws:rds:*:*:cluster:*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "rds:DatabaseEngine" : "neptune"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:autoscaled-reader*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingRDSClusterPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf RDS gewährt und CloudWatch.

`AWSApplicationAutoscalingRDSClusterPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Oktober 2017, 17:46 Uhr UTC
- Bearbeitete Zeit: 7. August 2018, 19:14 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingRDSClusterPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CreateDBInstance",
        "rds:DeleteDBInstance",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:ModifyDBCluster",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DescribeAlarms",
```

```
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "rds.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingSageMakerEndpointPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Zugriffsberechtigungen gewährt SageMaker und CloudWatch.

`AWSApplicationAutoscalingSageMakerEndpointPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. Februar 2018, 19:58 UTC
- Bearbeitete Zeit: 13. November 2023, 18:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingSageMakerEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMaker",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerCloudWatchUpdate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationAutoscalingWorkSpacesPoolPolicy

Beschreibung: Richtlinie, die Application Auto Scaling Berechtigungen für den Zugriff auf Amazon WorkSpaces und Amazon gewährt CloudWatch.

`AWSApplicationAutoscalingWorkSpacesPoolPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Juni 2024, 18:39 UTC
- Bearbeitungszeit: 17. Juni 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationAutoscalingWorkSpacesPoolPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WorkSpacesActionsOnAllPools",
      "Effect" : "Allow",
      "Action" : [
        "workspaces:DescribeWorkspacesPools",
        "workspaces:UpdateWorkspacesPool"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnAllAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchActionsOnTargetTrackingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:TargetTracking*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryAgentAccess

Beschreibung: Ermöglicht dem Discovery Agent den Zugriff auf die Registrierung beim AWS Application Discovery Service.

`AWSApplicationDiscoveryAgentAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationDiscoveryAgentAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2016, 21:38 UTC
- Bearbeitete Zeit: 24. Februar 2020, 22:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryAgentlessCollectorAccess

Beschreibung: Ermöglicht Application Discovery Service Agentless Collectors die auto Aktualisierung, Registrierung und Kommunikation mit dem Application Discovery Service

`AWSApplicationDiscoveryAgentlessCollectorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationDiscoveryAgentlessCollectorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 21:00 Uhr UTC
- Bearbeitete Zeit: 16. August 2022, 21:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryAgentlessCollectorAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:DescribeImages"
      ],
      "Resource" : "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:GetServiceBearerToken"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationDiscoveryServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf das Anzeigen und Markieren von Konfigurationselementen, die vom AWS Application Discovery Service verwaltet werden

`AWSApplicationDiscoveryServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationDiscoveryServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2016, 21:30 Uhr UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationDiscoveryServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentInstallationPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server verwendet wird. AWS Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSApplicationMigrationAgentInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationAgentInstallationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2022, 07:51 UTC
- Bearbeitete Zeit: 20. September 2022, 11:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server verwendet wird. AWS Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSApplicationMigrationAgentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationAgentPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 7. April 2021, 07:00 UTC
- Bearbeitete Zeit: 20. September 2022, 11:13 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationAgentPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationAgentPolicy_v2

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des AWS Replication Agents, der zusammen mit dem AWS Application Migration Service (MGN) verwendet wird, um externe Server zu AWS migrieren. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationAgentPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationAgentPolicy_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Juni 2022, 14:14 UTC
- Bearbeitungszeit: 6. Juni 2022, 14:14 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationAgentPolicy_v2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationConversionServerPolicy

Beschreibung: Diese Richtlinie ermöglicht dem Application Migration Service (MGN) - Konversionsserver, bei denen es sich um vom Application Migration Service gestartete EC2 Instanzen handelt, die Kommunikation mit dem MGN-Dienst. Eine IAM-Rolle mit dieser Richtlinie wird von MGN (als EC2 Instanzprofil) an die MGN Conversion Server angehängt, die bei Bedarf automatisch von MGN gestartet und beendet werden. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen. MGN Conversion Server werden vom Application Migration Service verwendet, wenn Benutzer Test- oder Cutover-Instances über die MGN-Konsole, CLI oder API starten möchten.

`AWSApplicationMigrationConversionServerPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationConversionServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 06:48 UTC
- Bearbeitete Zeit: 7. April 2021, 06:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationConversionServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationEC2Access

Beschreibung: Diese Richtlinie stellt die EC2 Amazon-Operationen bereit, die erforderlich sind, um den Application Migration Service (MGN) zu verwenden, um die migrierten Server als EC2 Instances zu starten. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationEC2Access` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 07:05 UTC
- Bearbeitete Zeit: 11. Februar 2025, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationEC2Access`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
```

```
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
```

```
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationFullAccess

Beschreibung: Diese Richtlinie gewährt allen Benutzern Zugriff auf den AWS Application Migration Service (MGN) sowie Berechtigungen zum Lesen von KMS-Schlüsselinformationen. APIs Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 06:56 UTC
- Bearbeitete Zeit: 2. Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationFullAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "mgn:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeTags",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor5",
```

```
      "Effect" : "Allow",
      "Action" : "iam:ListInstanceProfiles",
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithDrsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
```

```
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "drs:DisconnectSourceServer"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR" : "false"
        }
      }
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    },
    {
      "Sid" : "VisualEditor14",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor15",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*"
    },
    {
      "Sid" : "VisualEditor16",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
        "arn:aws:ssm:*:*:document/AWSMigration-*"
      ]
    },
    {
      "Sid" : "VisualEditor17",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor18",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSMigration-*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor19",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommands",
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor20",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationMGHAccess

Beschreibung: Diese Richtlinie ermöglicht es dem AWS Application Migration Service (MGN), Metadaten über den Fortschritt von Servern, die mithilfe von MGN migriert werden, an AWS Migration Hub (MGH) zu senden. MGN erstellt automatisch eine IAM-Rolle mit dieser angehängten Richtlinie und übernimmt diese Rolle. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationMGHAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationMGHAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 07:10 UTC
- Bearbeitete Zeit: 7. April 2021, 07:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationMGHAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationNetworkMigrationCustomResource

Beschreibung: Stellt Berechtigungen für die benutzerdefinierte Netzwerkmigrationsressource bereit

`AWSApplicationMigrationNetworkMigrationCustomResource`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationNetworkMigrationCustomResource` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. November 2025, 11:34 UTC
- Zeit bearbeitet: 5. November 2025, 11:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationCustomResource`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ModifyTGW",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationNetworkMigrationMultiAccount

Beschreibung: Bietet Berechtigungen zur Automatisierung der Migration VMware zur AWS Netzwerkinfrastruktur durch CloudFormation

`AWSApplicationMigrationNetworkMigrationMultiAccount`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationNetworkMigrationMultiAccount` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2025, 09:04 Uhr UTC
- Zeit bearbeitet: 10. November 2025, 09:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationNetworkMigrationMultiAccount`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2CFNReadonlyPrefixList",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:prefix-list/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "NetworkAnalyzer",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreatePermissionsByCFNNACL",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "CreatePermissionsByCFNNACLSN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CFNReadonly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNDescribe",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*"
    },
    {
```

```
      "Sid" : "CFNCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/Nmd*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CFNProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
```

```
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2PutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2ResourceSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2RequestSgTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "AnalyzerEC2SecurityGroupTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "EC2TagCFNSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
```

```
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateNatGateway",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateTGWVpcAttachmentSameOrg",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceOrgID" : "${aws:PrincipalOrgID}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CFNProvisionNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateVpc",
        "ec2:CreateTransitGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:transit-gateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworking",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAcl",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagRouting",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNAT",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagTGWAttachment",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
```

```
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreatePermissionsByRequestTagNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    },
    {
      "Sid" : "DeleteENI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
```

```
    },
    {
      "Sid" : "CreatePermissionsByRequestTagInsights",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInsightsPath"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-insights-path/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EC2TagCFN",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
```

```
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "ec2:CreateAction" : [
            "CreateTransitGatewayVpcAttachment",
            "CreateTransitGatewayRouteTableAnnouncement",
            "CreateTransitGatewayRouteTable",
            "CreateTransitGatewayRoute",
            "CreateTransitGatewayPrefixListReference",
            "CreateTransitGatewayPolicyTable",
            "CreateTransitGatewayPeeringAttachment",
            "CreateTransitGatewayConnectPeer",
            "CreateTransitGatewayConnect",
            "CreateTransitGateway",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateSubnet",
            "CreateNetworkAcl",
            "CreateRouteTable",
            "CreateNetworkInterface",
            "CreateNetworkInsightsPath",
            "CreateNetworkInsightsAccessScope",
            "CreateLaunchTemplate",
            "AllocateAddress",
            "StartNetworkInsightsAnalysis",
            "CreateVpc"
          ]
        }
      }
    },
    {
      "Sid" : "deployerWorkload",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "putParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "deleteParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:ListTagsForResource",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/network-migration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ramTAgReource",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareTransitGateway",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "Bool" : {
```

```
          "ram:RequestedAllowsExternalPrincipals" : "false"
        }
      }
    },
    {
      "Sid" : "AssociateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "ram:RequestedResourceType" : [
            "ec2:TransitGateway",
            "ssm:Parameter"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateResourceShareWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "AllowGetResourceShares",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*"
    },
    {
      "Sid" : "CreateCustomResourceLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/network-migration-modify-tgw*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OperationsCustomResourceLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:network-migration*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CreateRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSApplicationMigrationService",
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassGetRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OperationsRoleCustomResource",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AttachCustomResourceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/Nmd*modifyTransitGateway*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/
AWSApplicationMigrationNetworkMigrationCustomResource"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "MGNCFNBasedResourcesProvision",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
        "ec2:AssociateNatGatewayAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteNetworkInsightsAnalysis",
        "ec2:DeleteNetworkInsightsPath",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteSubnet",
```

```
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DeleteVolume",
        "ec2:DeleteVpc",
        "ec2:DetachInternetGateway",
        "ec2:DetachVolume",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateNatGatewayAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyLaunchTemplate",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:ModifyVolume",
        "ec2:ModifyVpcAttribute",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:StartNetworkInsightsAnalysis"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway/*",
        "arn:aws:ec2:*:*:transit-gateway-policy-table/*",
        "arn:aws:ec2:*:*:transit-gateway-connect-peer/*",
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:network-insights-path/*",
```

```
        "arn:aws:ec2:*:*:network-insights-access-scope-analysis/*",
        "arn:aws:ec2:*:*:network-insights-access-scope/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:elastic-ip/*",
        "arn:aws:ec2:*:*:network-insights-analysis/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AnalyzerENIResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSApplicationMigrationService"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt allen öffentlichen Bereichen APIs des Application Migration Service (MGN), die nur lesbar sind, sowie einigen schreibgeschützten APIs anderen AWS Diensten, die erforderlich sind, um die MGN-Konsole vollständig schreibgeschützt nutzen zu können. Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu.

`AWSApplicationMigrationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. April 2021, 07:15 UTC
- Bearbeitete Zeit: 20. März 2023, 08:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationReplicationServerPolicy

Beschreibung: Diese Richtlinie ermöglicht es den Application Migration Service (MGN) Replication Servern, bei denen es sich um vom Application Migration Service gestartete EC2 Instances handelt, mit dem MGN Service zu kommunizieren und EBS-Snapshots in Ihrem zu erstellen. AWS-Konto Eine IAM-Rolle mit dieser Richtlinie wird (als EC2 Instanzprofil) vom Application Migration Service den MGN Replication Servern zugewiesen, die bei Bedarf automatisch von MGN gestartet und beendet werden. MGN Replication Server werden verwendet, um im Rahmen des mit MGN verwalteten Migrationsprozesses die Datenreplikation von Ihren externen Servern zu AWS erleichtern. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSApplicationMigrationReplicationServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationReplicationServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. April 2021, 07:21 UTC
- Bearbeitete Zeit: 7. April 2021, 07:21 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSApplicationMigrationReplicationServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationServiceEc2InstancePolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der vom AWS Application Migration Service (AWS MGN) zur Migration von Quellservern verwendet wird, die auf EC2 (regionsübergreifend oder azübergreifend) ausgeführt werden. Eine IAM-Rolle mit dieser Richtlinie sollte den Instances (als EC2 Instanzprofil) zugewiesen werden. EC2

`AWSApplicationMigrationServiceEc2InstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationServiceEc2InstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2023, 13:19 UTC
- Bearbeitete Zeit: 03. Januar 2024, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationServiceEc2InstancePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MgnAgentInstallation",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MgnAgentReplication",
      "Effect" : "Allow",
      "Action" : [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:source-server/*"
    },
    {
      "Sid" : "MgnSourceServerTagResource",
      "Effect" : "Allow",
      "Action" : "mgn:TagResource",
      "Resource" : "arn:aws:mgn:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "mgn:CreateAction" : "RegisterAgentForMgn"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationServiceRolePolicy

Beschreibung: Ermöglicht dem AWS Anwendungsmigrationsdienst, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AWSApplicationMigrationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. April 2021, 06:43 UTC
- Bearbeitete Zeit: 16. März 2025, 10:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSApplicationMigrationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgn:ListTagsForResource",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
```

```
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:aws:organizations::*:account/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
```

```
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationSSMAccess

Beschreibung: Diese Richtlinie bietet Zugriff auf Amazon SSM-Operationen, die für die Verwendung des Application Migration Service (MGN) zur Ausführung benutzerdefinierter SSM-Dokumente nach der Migration erforderlich sind. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSApplicationMigrationSSMAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationSSMAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 09:29 UTC
- Bearbeitete Zeit: 2. Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationSSMAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "mgn.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSApplicationMigrationVCenterClientPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS VCenter Clients, der zusammen mit dem AWS Application Migration Service (MGN) zur Migration externer Server verwendet wird. AWS Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu, deren Anmeldeinformationen Sie bei der AWS VCenter Installation des Clients angeben.

`AWSApplicationMigrationVCenterClientPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSApplicationMigrationVCenterClientPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. November 2021, 12:53 Uhr UTC

- Bearbeitete Zeit: 8. November 2021, 12:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSApplicationMigrationVCenterClientPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",
        "mgn:SendVcenterClientMetricsForMgn",
        "mgn:DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
      ],
      "Resource" : "arn:aws:mgn:*:*:vcenter-client/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshEnvoyAccess

Beschreibung: App Mesh Envoy-Richtlinie für den Zugriff auf die Konfiguration des virtuellen Knotens.

`AWSAppMeshEnvoyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppMeshEnvoyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Juli 2019, 21:29 Uhr UTC
- Bearbeitete Zeit: 3. Juli 2019, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS App Mesh APIs und Management Console.

`AWSAppMeshFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppMeshFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2019, 17:50 Uhr UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appmesh.amazonaws.com/
AWSServiceRoleForAppMesh",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "appmesh.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStack*",
```

```
        "cloudformation:UpdateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshPreviewEnvoyAccess

Beschreibung: App Mesh Preview Envoy-Richtlinie für den Zugriff auf die Konfiguration des virtuellen Knotens.

`AWSAppMeshPreviewEnvoyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppMeshPreviewEnvoyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. August 2019, 23:32 UTC
- Zeit bearbeitet: 5. August 2019, 23:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshPreviewEnvoyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh-preview:StreamAggregatedResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshPreviewServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von AWS App Mesh verwendet oder verwaltet werden

`AWSAppMeshPreviewServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juni 2019, 19:07 UTC
- Bearbeitete Zeit: 21. August 2019, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshPreviewServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS App Mesh APIs und Management Console.

`AWSAppMeshReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppMeshReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 16. April 2019, 17:51 UTC
- Bearbeitete Zeit: 7. Januar 2021, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppMeshReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appmesh:Describe*",
        "appmesh:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSAppMesh-GettingStarted-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "acm:DescribeCertificate",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:ListNamespaces",
        "servicediscovery:ListServices",
        "servicediscovery:ListInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppMeshServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von verwendet oder verwaltet werden AWS AppMesh

`AWSAppMeshServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Juni 2019, 18:30 Uhr UTC

- Bearbeitete Zeit: 10. Oktober 2023, 16:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppMeshServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudMapServiceDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ACMCertificateVerification",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerFullAccess

Beschreibung: Erteilt Berechtigungen für alle App Runner-Aktionen.

`AWSAppRunnerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppRunnerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2022, 04:02 UTC
- Bearbeitete Zeit: 11. Januar 2022, 04:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/apprunner.amazonaws.com/
AWSServiceRoleForAppRunner",
```

```
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "apprunner.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRunnerAdminAccess",
      "Effect" : "Allow",
      "Action" : "apprunner:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerReadOnlyAccess

Beschreibung: Erteilt Berechtigungen zum Auflisten und Anzeigen von Details zu App Runner-Ressourcen.

`AWSAppRunnerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppRunnerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Februar 2022, 21:24 UTC
- Bearbeitete Zeit: 24. Februar 2022, 21:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppRunnerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apprunner:List*",
        "apprunner:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppRunnerServicePolicyForECRAccess

Beschreibung: AWS App Runner-Servicerichtlinie, die Leseberechtigungen für Amazon ECR-Ressourcen im Kundenkonto gewährt. Verwenden Sie es in einer Rolle, die bei der Erstellung oder Aktualisierung eines App Runner-Service an App Runner übergeben wird.

`AWSAppRunnerServicePolicyForECRAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppRunnerServicePolicyForECRAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Mai 2021, 19:17 UTC
- Bearbeitete Zeit: 14. Mai 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppRunnerServicePolicyForECRAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncAdministrator

Beschreibung: Bietet Administratorzugriff auf den AppSync Dienst, reicht jedoch nicht aus, um über die Konsole darauf zuzugreifen.

`AWSAppSyncAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppSyncAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. März 2018, 21:20 Uhr UTC
- Zeit bearbeitet: 4. November 2019, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncAdministrator`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "appsync.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "appsync.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/appsync.amazonaws.com/
AWSServiceRoleForAppSync*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncInvokeFullAccess

Beschreibung: Bietet vollen Aufrufzugriff auf den AppSync Dienst — sowohl über die Konsole als auch unabhängig

`AWSAppSyncInvokeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppSyncInvokeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. März 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 20. März 2018, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncInvokeFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:GetGraphqlApi",
        "appsync:ListGraphqlApis",
        "appsync:ListApiKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncPushToCloudWatchLogs

Beschreibung: Ermöglicht AppSync das Senden von Protokollen an das CloudWatch Benutzerkonto.

`AWSAppSyncPushToCloudWatchLogs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppSyncPushToCloudWatchLogs` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 9. April 2018, 19:38 UTC
- Bearbeitete Zeit: 9. April 2018, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSAppSyncPushToCloudWatchLogs`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncSchemaAuthor

Beschreibung: Ermöglicht den Zugriff zum Erstellen, Aktualisieren und Abfragen des Schemas.

`AWSAppSyncSchemaAuthor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAppSyncSchemaAuthor` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. März 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 1. Februar 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAppSyncSchemaAuthor`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "appsync:GraphQL",
        "appsync:CreateResolver",
        "appsync:CreateType",
        "appsync:DeleteResolver",
        "appsync:DeleteType",
        "appsync:GetResolver",
        "appsync:GetType",
        "appsync:GetDataSource",
        "appsync:GetSchemaCreationStatus",
        "appsync:GetIntrospectionSchema",
        "appsync:GetGraphqlApi",
        "appsync:ListTypes",
        "appsync:ListApiKeys",
        "appsync:ListResolvers",
        "appsync:ListDataSources",
        "appsync:ListGraphqlApis",
        "appsync:StartSchemaCreation",
        "appsync:UpdateResolver",
        "appsync:UpdateType",
        "appsync:TagResource",
        "appsync:UntagResource",
        "appsync:ListTagsForResource",
        "appsync:CreateFunction",
        "appsync:UpdateFunction",
        "appsync:GetFunction",
        "appsync:DeleteFunction",
```

```
        "appsync:ListFunctions",
        "appsync:ListResolversByFunction",
        "appsync:EvaluateMappingTemplate",
        "appsync:EvaluateCode"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAppSyncServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die verwendet oder verwaltet werden von AppSync

`AWSAppSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Januar 2020, 19:56 UTC
- Bearbeitete Zeit: 21. Januar 2020, 19:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAppSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingTargets",
        "xray:GetSamplingRules",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactAccountSync

Beschreibung: Ermöglicht AWS Artifact den schreibgeschützten Zugriff auf Operationen in Organizations. AWS

`AWSArtifactAccountSync`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSArtifactAccountSync` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. April 2018, 23:04 UTC
- Bearbeitete Zeit: 10. April 2018, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSArtifactAccountSync`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactAgreementsFullAccess

Beschreibung: Diese Richtlinie gewährt volle Rechte zum Auflisten, Herunterladen, Akzeptieren und Kündigen von AWS Artifact-Vereinbarungen. Sie umfasst auch Berechtigungen zum Auflisten und Aktivieren AWS des Zugriffs auf Dienste im Organisationsdienst sowie zur Beschreibung der Organisationsdetails. Darüber hinaus bietet die Richtlinie die Möglichkeit, zu überprüfen, ob die erforderliche dienstbezogene Rolle vorhanden ist, und eine zu erstellen, falls dies nicht der Fall ist

`AWSArtifactAgreementsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSArtifactAgreementsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2024, 19:36 UTC
- Bearbeitete Zeit: 16. Oktober 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource" : "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid" : "CustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetRoleToCheckForRoleExistence",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid" : "EnableServiceTrust",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EnableServiceTrustForArtifact",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "aws-artifact-account-sync.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactAgreementsReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt Lesezugriff, um die AWS Artifact-Serviceverträge aufzulisten und die akzeptierten Vereinbarungen herunterzuladen. Sie umfasst auch die Erlaubnis, die Organisationsdetails aufzulisten und zu beschreiben. Darüber hinaus bietet die Richtlinie die Möglichkeit, zu überprüfen, ob die erforderliche dienstbezogene Rolle vorhanden ist.

`AWSArtifactAgreementsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSArtifactAgreementsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2024, 19:36 UTC
- Bearbeitete Zeit: 22. November 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactAgreementsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListAgreementsActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetCustomerAgreementActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetCustomerAgreement"
      ],
      "Resource" : "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid" : "AWSOrganizationActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactReportsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Artifact-Serviceberichte.

`AWSArtifactReportsReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSArtifactReportsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 02. Januar 2024, 22:42 UTC
- Bearbeitete Zeit: 16. Dezember 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSArtifactReportsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactReportActions",
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports",
        "artifact:ListReportVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSArtifactServiceRolePolicy

Beschreibung: Ermöglicht AWS Artifact, Informationen über eine Organisation über den AWS Organisationsdienst zu sammeln.

`AWSArtifactServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. August 2023, 20:27 UTC
- Bearbeitete Zeit: 21. August 2023, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSArtifactServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAuditManagerAdministratorAccess

Beschreibung: Bietet Administratorzugriff, um AWS Audit Manager zu aktivieren oder zu deaktivieren, Einstellungen zu aktualisieren und Bewertungen, Kontrollen und Frameworks zu verwalten

`AWSAuditManagerAdministratorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSAuditManagerAdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2020, 20:02 Uhr UTC
- Bearbeitete Zeit: 15. Mai 2024, 23:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSAuditManagerAdministratorAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOnlyAuditManagerIntegration",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "auditmanager.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "auditmanager.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMAccessManageSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:UpdateRoleDescription",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "ForAllValues:StringEquals" : {
```

```
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ControlCatalogAccess",
      "Effect" : "Allow",
      "Action" : [
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAuditManagerServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von AWS Audit Manager verwendet oder verwaltet werden

`AWSAuditManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Dezember 2020, 15:12 Uhr UTC
- Bearbeitete Zeit: 24. September 2024, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAuditManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:ListBackupPlans",
        "backup:ListRecoveryPointsByResource",
        "bedrock:GetCustomModel",
        "bedrock:GetFoundationModel",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListCustomModels",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListModelCustomizationJobs",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cognito-idp:DescribeUserPool",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:ListDiscoveredResources",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeBackup",
```

```
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTable",
        "dynamodb:ListBackups",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:GetLaunchTemplateData",
        "ec2:DescribeAddresses",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ecs:DescribeClusters",
        "eks:DescribeAddonVersions",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeServiceUpdates",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSslPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
```

```
        "elasticmapreduce:ListSecurityConfigurations",
        "events:DescribeRule",
        "events:ListConnections",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRules",
        "firehose:ListDeliveryStreams",
        "fsx:DescribeFileSystems",
        "guardduty:ListDetectors",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccessKeyLastUsed",
        "iam:GetCredentialReport",
        "iam:GetGroupPolicy",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupsForUser",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListOpenIdConnectProviders",
        "iam:ListPolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSamlProviders",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListAccessKeys",
        "iam:ListAttachedRolePolicies",
        "iam:ListMfaDeviceTags",
        "iam:ListMfaDevices",
        "kafka:ListClusters",
        "kafka:ListKafkaVersions",
        "kinesis:ListStreams",
        "kms:DescribeKey",
```

```
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListGrants",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "license-manager:ListAssociationsForLicenseConfiguration",
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListUsageForLicenseConfiguration",
        "logs:DescribeDestinations",
        "logs:DescribeExportTasks",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:FilterLogEvents",
        "logs:GetDataProtectionPolicy",
        "es:DescribeDomains",
        "es:DescribeDomain",
        "es:DescribeDomainConfig",
        "es:ListDomainNames",
        "organizations:DescribeOrganization",
        "organizations:DescribePolicy",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeLoggingStatus",
        "route53:GetQueryLoggingConfig",
        "sagemaker:DescribeAlgorithm",
        "sagemaker:DescribeFlowDefinition",
        "sagemaker:DescribeHumanTaskUi",
        "sagemaker:DescribeModelBiasJobDefinition",
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeLabelingJob",
        "sagemaker:DescribeModel",
```

```
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListLabelingJobs",
        "sagemaker:ListModels",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListMonitoringAlerts",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListUserProfiles",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:ListAllMyBuckets",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecrets",
        "securityhub:DescribeStandards",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:ListQueues",
        "waf-regional:GetRule",
        "waf-regional:GetWebAcl",
        "waf:GetRule",
        "waf:GetRuleGroup",
        "waf:ListActivatedRulesInRuleGroup",
        "waf:ListWebAcls",
        "wafv2:ListWebAcls",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:ListRuleGroups",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListWebACLs",
        "waf-regional:ListRules",
        "waf:ListRuleGroups",
        "waf:ListRules"
      ],
      "Resource" : "*",
```

```
      "Sid" : "APIsAccess"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLogging",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEventsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
      "Condition" : {
        "StringEquals" : {
          "events:detail-type" : "Security Hub Findings - Imported"
        },
        "Null" : {
          "events:source" : "false"
        },
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.securityhub"
          ]
        }
      }
    },
    {
      "Sid" : "EventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSAutoScalingPlansEC2AutoScalingPolicy

Beschreibung: Richtlinie, die AWS Auto Scaling berechtigt, die Kapazität regelmäßig zu prognostizieren und geplante Skalierungsaktionen für Auto Scaling Scaling-Gruppen in einem Skalierungsplan zu generieren

`AWSAutoScalingPlansEC2AutoScalingPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. August 2018, 22:46 Uhr UTC
- Bearbeitete Zeit: 23. August 2018, 22:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSAutoScalingPlansEC2AutoScalingPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:BatchPutScheduledUpdateGroupAction",
        "autoscaling:BatchDeleteScheduledAction"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupAuditAccess

Beschreibung: Diese Richtlinie gewährt Benutzern die Erlaubnis, Kontrollen und Frameworks zu erstellen, die ihre Erwartungen an AWS Backup-Ressourcen und -Aktivitäten definieren, und AWS Backup-Ressourcen und -Aktivitäten anhand ihrer definierten Kontrollen und Frameworks zu überprüfen. Diese Richtlinie gewährt AWS Config und ähnlichen Diensten die Erlaubnis, die Erwartungen der Benutzer bei der Durchführung der Audits zu beschreiben. Diese Richtlinie gewährt auch Berechtigungen zur Übermittlung von Auditberichten an S3 und ähnliche Dienste und ermöglicht es Benutzern, ihre Auditberichte zu finden und zu öffnen.

`AWSBackupAuditAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupAuditAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. August 2021, 01:02 UTC

- Bearbeitete Zeit: 10. April 2023, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupAuditAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateFramework",
        "backup:UpdateFramework",
        "backup:ListFrameworks",
        "backup:DescribeFramework",
        "backup:DeleteFramework",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:CreateReportPlan",
        "backup:UpdateReportPlan",
        "backup:ListReportPlans",
        "backup:DescribeReportPlan",
        "backup:DeleteReportPlan",
        "backup:StartReportJob",
        "backup:ListReportJobs",
        "backup:DescribeReportJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeComplianceByConfigRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupDataTransferAccess

Beschreibung: Diese Richtlinie ermöglicht es dem AWS Backint-Agenten, die Backup-Datenübertragung mit der AWS Backup-Speicherebene abzuschließen. Hängen Sie diese Richtlinie an Rollen an, die von EC2 Instanzen übernommen werden, auf denen SAP HANA mit dem Backint-Agenten ausgeführt wird.

`AWSBackupDataTransferAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupDataTransferAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 22:48 UTC
- Bearbeitete Zeit: 10. November 2022, 22:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupDataTransferAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup-storage:StartObject",
        "backup-storage:PutChunk",
        "backup-storage:GetChunk",
        "backup-storage:ListChunks",
        "backup-storage:ListObjects",
        "backup-storage:GetObjectMetadata",
        "backup-storage:NotifyObjectComplete"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupFullAccess

Beschreibung: Diese Richtlinie richtet sich an Backup-Administratoren und gewährt vollen Zugriff auf AWS Backup-Operationen, darunter das Erstellen oder Bearbeiten von Backup-Plänen, das Zuweisen von AWS Ressourcen zu Backup-Plänen, das Löschen von Backups und das Wiederherstellen von Backups.

`AWSBackupFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2019, 22:21 Uhr UTC
- Bearbeitete Zeit: 20. November 2025, 03:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupFullAccess`

Version der Richtlinie

Richtlinienversion: v22 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AwsBackupStorageAllAccessPermissions",
      "Effect" : "Allow",
      "Action" : "backup-storage:*",
      "Resource" : "*"
    },
    {
      "Sid" : "RdsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RdsDeletePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDbPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDbDeleteBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EfsFileSystemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
```

```
    },
    {
      "Sid" : "Ec2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2DeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ResourceGroupTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayGatewayStarPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AwsOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:backup:backup-vault"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringLike" : {
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemManagerCommandPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SystemManagerSendCommandPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems",
        "fsx:DescribeBackups",
        "fsx:DescribeVolumes",
        "fsx:DescribeStorageVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
```

```
      "Resource" : "arn:aws:fsx:*:*:backup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DirectoryServicePermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "IamCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "backup.amazonaws.com",
            "restore-testing.backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BackupGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:AssociateGatewayToServer",
        "backup-gateway:CreateGateway",
        "backup-gateway:DeleteGateway",
        "backup-gateway:DeleteHypervisor",
        "backup-gateway:DisassociateGatewayFromServer",
        "backup-gateway:ImportHypervisorConfiguration",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup-gateway:PutMaintenanceStartTime",
```

```
        "backup-gateway:TagResource",
        "backup-gateway:TestHypervisorConfiguration",
        "backup-gateway:UntagResource",
        "backup-gateway:UpdateGatewayInformation",
        "backup-gateway:UpdateHypervisor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayHypervisorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:PutHypervisorPropertyMappings",
        "backup-gateway:StartVirtualMachinesMetadataSync"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayVirtualMachinePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:PutBandwidthRateLimitSchedule"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "TimestreamDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListTables",
        "timestream:ListDatabases"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeletetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SystemsManagerForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceAccessManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Beschreibung: AWS BackupGateway Erlaubt die Erlaubnis, die Metadaten virtueller Maschinen in Ihrem Namen zu synchronisieren

`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. Dezember 2022, 19:43 UTC
- Bearbeitete Zeit: 15. Dezember 2022, 19:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListVmTags",
      "Effect" : "Allow",
      "Action" : [
```

```
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "VMTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:TagResource",
        "backup-gateway:UntagResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupGuardDutyRolePolicyForScans

Beschreibung: GuardDuty Erlaubt das Lesen Ihrer AWS Backup-Wiederherstellungspunkte für Malware-Scans

`AWSBackupGuardDutyRolePolicyForScans`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupGuardDutyRolePolicyForScans` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 20. November 2025, 03:34 UTC
- Bearbeitete Zeit: 20. November 2025, 03:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupGuardDutyRolePolicyForScans`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:ListChangedBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "CreateGrantForEncryptedVolumeCreation",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:guardduty:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "CreateGrant",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "CreateGrantForReEncryptAndEBSDirect",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : "snap-*",
          "kms:ViaService" : [
            "guardduty.*.amazonaws.com",
            "backup.*.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "RetireGrant",
            "DescribeKey"
```

```
          ]
        },
        "Null" : {
          "kms:GrantOperations" : "false"
        }
      }
    },
    {
      "Sid" : "DescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ShareSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        },
        "StringLike" : {
          "aws:ResourceTag/aws:backup:source-resource" : "*"
        }
      }
    },
    {
      "Sid" : "ShareSnapshotKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:ebs:id" : [
            "vol-*",
            "snap-*"
          ],
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CreateBackupAccessPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "ReadAndDeleteBackupAccessPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupAccessPoint",
        "backup:DeleteBackupAccessPoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupRecoveryPointApiPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*"
    },
    {
      "Sid" : "DecryptKMSEncryptedDataByAWSBackup",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:aws:backup:backup-vault" : "*",
          "kms:ViaService" : "backup.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupOperatorAccess

Beschreibung: Diese Richtlinie gewährt Benutzern die Berechtigung, AWS Ressourcen Backup-Plänen zuzuweisen, On-Demand-Backups zu erstellen und Backups wiederherzustellen. Diese Richtlinie erlaubt es dem Benutzer nicht, Backup-Pläne zu erstellen oder zu bearbeiten oder geplante Backups zu löschen, nachdem sie erstellt wurden.

`AWSBackupOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2019, 22:23 Uhr UTC
- Bearbeitete Zeit: 20. November 2025, 03:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOperatorAccess`

Version der Richtlinie

Richtlinienversion: v20 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsBackupAllAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:CreateBackupSelection",
        "backup:DeleteBackupSelection",
        "backup:StartBackupJob",
        "backup:StartRestoreJob",
        "backup:StartCopyJob",
        "backup:StartScanJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:describeDBEngineVersions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describeDBSubnetGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
```

```
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBAccess",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListBackups",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSAccess",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeFilesystems"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "EC2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:describeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "StorageGatewaySCSIAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListGateways"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "StorageGatewayDiskReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListLocalDisks"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayVolumeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackup*",
        "arn:aws:iam::*:role/*AWSBackup*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMComandAccess",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
```

```
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "FSXDescribeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FSxFileAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FSxVolumeAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*/*"
    },
    {
      "Sid" : "FSxMachineAccess",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeStorageVirtualMachines",
      "Resource" : "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
    },
    {
      "Sid" : "DirectoryServiceAccess",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "BackupGatewayListAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "BackupGatewayHypervisorAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "BackupGatewayMachineAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetVirtualMachine"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "BackupGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:gateway/*"
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamListAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
```

```
      "Sid" : "TimestreamDescribeAccess",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "RedshiftAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeSnapshotSchedules"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift:*:*:subnetgroup:*",
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:snapshotschedule:*"
      ]
    },
    {
      "Sid" : "RedshiftOptionsAccess",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeNodeConfigurationOptions",
        "redshift:DescribeOrderableClusterOptions",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterTracks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "CloudFormationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "SAPAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SAPDatabaseAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "IamPassRolePermissionsForGuardDuty",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*AwsBackupGuardDuty*",
        "arn:aws:iam::*:role/*AWSBackupGuardDuty*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupOrganizationAdminAccess

Beschreibung: Diese Richtlinie richtet sich an Backup-Administratoren, die kontoübergreifendes Backup-Management verwenden, um Backups für das Unternehmen zu verwalten.

`AWSBackupOrganizationAdminAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSBackupOrganizationAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2020, 16:23 UTC
- Zeit bearbeitet: 18. November 2022, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupOrganizationAdminAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DisableAWSServiceAccess",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:AttachPolicy",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListPolicies",
        "organizations:EnablePolicyType",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:PolicyType" : [
            "BACKUP_POLICY"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupRestoreAccessForSAPHANA

Beschreibung: Bietet die AWS Backup-Berechtigung zum Wiederherstellen eines Backups von SAP HANA auf Amazon EC2

`AWSBackupRestoreAccessForSAPHANA`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupRestoreAccessForSAPHANA` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2022, 22:43 UTC
- Zeit bearbeitet: 10. November 2022, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupRestoreAccessForSAPHANA`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:Get*",
        "backup:List*",
        "backup:Describe*",
        "backup:StartBackupJob",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:RestoreDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupSearchOperatorAccess

Beschreibung: Die Suchoperatorrolle hat Zugriff auf die Erstellung von Backup-Indizes und die Erstellung von Suchvorgängen für indexierte Backup-Metadaten. Diese Richtlinie enthält die erforderlichen Berechtigungen für diese Suchoperatorfunktionen.

`AWSBackupSearchOperatorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupSearchOperatorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Februar 2025, 21:52 UTC
- Bearbeitete Zeit: 25. März 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupSearchOperatorAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "StartSearchAndListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchJob",
        "backup-search:ListSearchJobs",
        "backup-search:ListSearchResultExportJobs",
        "backup:ListIndexedRecoveryPointsForSearch"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BackupSearchRecoveryPointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:SearchRecoveryPoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:backup:*:*:recovery-point:*"
      ]
    },
    {
      "Sid" : "SearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-search:StartSearchResultExportJob",
        "backup-search:StopSearchJob",
        "backup-search:GetSearchJob",
        "backup-search:GetSearchResultExportJob",
        "backup-search:ListSearchJobResults",
        "backup-search:ListSearchJobBackups"
      ],
      "Resource" : [
        "arn:aws:backup-search:*:*:search-job/*",
        "arn:aws:backup-search:*:*:search-export-job/*"
      ]
    },
    {
      "Sid" : "KMSDataKeyForSearchAndExportPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:backup-search:search-job"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "backup.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceLinkedRolePolicyForBackup

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceLinkedRolePolicyForBackup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Juni 2020, 23:08 UTC
- Zeit bearbeitet: 10. November 2025, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v21 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EFSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
        }
      }
    },
    {
      "Sid" : "DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "tag:GetResources",
        "elasticfilesystem:DescribeFileSystems",
        "dynamodb:ListTables",
        "storagegateway:ListVolumes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstances",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SnapshotCopyTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Sid" : "EC2CreateBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AWSBackupManagedResource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2RDSDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeImages",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBClusterSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CopyImage",
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotTier"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSBackupManagedResource" : "false"
        }
      }
    },
    {
      "Sid" : "RDSInstanceAndSnashotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBSnapshot",
        "rds:DeleteDBSnapshot",
        "rds:DeleteDBInstanceAutomatedBackup"
      ],
      "Resource" : "arn:aws:rds:*:*:snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:CopyDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
    },
    {
      "Sid" : "RDSSnapshotTenantDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot-tenant-database:awsbackup:*"
      ]
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "KMSGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "fsx.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CopyBackup",
        "fsx:TagResource",
        "fsx:DescribeBackups",
```

```
        "fsx:DeleteBackup"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamoDBDeletePermissions",
      "Effect" : "Allow",
      "Action" : "dynamodb:DeleteBackup",
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "BackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListVirtualMachines"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListTagsForBackupGateway",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
```

```
    {
      "Sid" : "EventBridgePermissions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:UpdateHANABackupSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:DescribeDatabase",
        "timestream:DescribeTable",
        "timestream:GetAwsBackupStatus",
        "timestream:GetAwsRestoreStatus"
      ],
```

```
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
```

```
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessDeleteSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudformationStackPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/*"
      ]
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrgsListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "backup.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceLinkedRolePolicyForBackupTest

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceLinkedRolePolicyForBackupTest`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Mai 2020, 17:37 UTC
- Bearbeitete Zeit: 12. Mai 2020, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBackupServiceLinkedRolePolicyForBackupTest`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect" : "Allow",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:elasticfilesystem:default-backup" : "enabled"
```

```
        }
      }
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForBackup

Beschreibung: Bietet die AWS Backup-Berechtigung, um in Ihrem Namen Backups für alle AWS Dienste zu erstellen

`AWSBackupServiceRolePolicyForBackup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForBackup` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. Januar 2019, 21:01 UTC
- Zeit bearbeitet: 10. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForBackup`

Version der Richtlinie

Richtlinienversion: v23 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:CreateBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeBackup",
        "dynamodb:DeleteBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "DynamoDBBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
```

```
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:CopyDBClusterSnapshot",
        "rds:DescribeDBClusterAutomatedBackups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RDSInstanceAutomatedBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBInstanceAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:auto-backup:*"
    },
    {
      "Sid" : "RDSClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RDSClusterBackupPermissions",
      "Effect" : "Allow",
      "Action" : "rds:DeleteDBClusterAutomatedBackup",
      "Resource" : "arn:aws:rds:*:*:cluster-auto-backup:*"
    },
    {
      "Sid" : "RDSModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:ModifyDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "RDSBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBSnapshot",
```

```
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "RDSClusterModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DeleteDBClusterSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Sid" : "StorageGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "EBSCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2CopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSTagAndDeletePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSnapshotTierStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:image/*"
    },
    {
      "Sid" : "EC2ModifyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotTierPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "BackupVaultPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource" : "arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Sid" : "BackupVaultCopyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:CopyFromBackupVault"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
```

```
      "Sid" : "EBSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSDynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "KMSEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:ebs:id"
        }
      }
    },
    {
      "Sid" : "GetResourcesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSendPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
```

```
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxCreateBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:CreateBackup",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeFileSystems",
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeVolumes",
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxListTagsPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:ListTagsForResource",
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DeleteBackup",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
```

```
    {
      "Sid" : "FsxResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "DynamodbBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:StartAwsBackupJob",
        "dynamodb:ListTagsOfResource"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "BackupGatewayBackupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:vm/*"
    },
    {
      "Sid" : "CloudformationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*/*"
    },
    {
      "Sid" : "RedshiftCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "redshift:CreateClusterSnapshot",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DeleteClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "RedshiftResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:CreateTags"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateSnapshot"
```

```
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*",
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftServerlessGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessListPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:StartAwsBackupJob",
        "timestream:GetAwsBackupStatus",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListTagsForResource",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSAPPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:GetOperation",
        "ssm-sap:ListDatabases"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SSMSAPResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:BackupDatabase",
        "ssm-sap:UpdateHanaBackupSettings",
        "ssm-sap:GetDatabase",
        "ssm-sap:ListTagsForResource"
      ],
      "Resource" : "arn:aws:ssm-sap:*:*:*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "DSQLResourcePermissionsForBackup",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartBackupJob",
        "dsql:GetBackupJob",
        "dsql:StopBackupJob",
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDSQLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dsql.*.amazonaws.com"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:dsql:ClusterId"
        }
      }
    },
    {
      "Sid" : "EKSClusterConfigurationBackup",
      "Effect" : "Allow",
      "Action" : [
        "eks:ListClusters",
        "eks:ListTagsForResource",
        "eks:DescribeCluster",
        "eks:ListAddons",
        "eks:DescribeAddon",
        "eks:ListNodegroups",
        "eks:DescribeNodegroup",
        "eks:ListPodIdentityAssociations",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListFargateProfiles",
        "eks:DescribeFargateProfile",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBackupAccessEntry",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateAccessEntry"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "AssociateBackupAccessPolicy",
```

```
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForBackup",
          "eks:accessScope" : "cluster"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForIndexing

Beschreibung: Richtlinie mit den erforderlichen Berechtigungen für AWS Backup zum Indizieren von Wiederherstellungspunkten.

`AWSBackupServiceRolePolicyForIndexing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForIndexing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 17. Dezember 2024, 18:37 UTC
- Bearbeitete Zeit: 17. Dezember 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForIndexing`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
```

```
    },
    {
      "Sid" : "KMSDataKeyForEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForItemRestores

Beschreibung: Richtlinie mit Berechtigungen, die AWS Backup benötigt, um einzelne Elemente in einem Wiederherstellungspunkt wiederherzustellen

`AWSBackupServiceRolePolicyForItemRestores`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForItemRestores` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Dezember 2024, 18:37 UTC
- Bearbeitete Zeit: 17. Dezember 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForItemRestores`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/*"
    },
    {
      "Sid" : "EBSDirectReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:ListSnapshotBlocks",
```

```
        "ebs:GetSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Sid" : "S3ReadonlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForFileLevelRestore",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSDataKeyForS3AndEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
```

```
            "ec2.*.amazonaws.com",
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForRestores

Beschreibung: Bietet die AWS Backup-Berechtigung, in Ihrem Namen wiederherzustellende AWS Dienste durchzuführen. Diese Richtlinie umfasst Berechtigungen zum Erstellen und Löschen von AWS Ressourcen wie EBS-Volumes, RDS-Instances und EFS-Dateisystemen, die Teil des Wiederherstellungsprozesses sind.

`AWSBackupServiceRolePolicyForRestores`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForRestores` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Januar 2019, 00:23 UTC
- Zeit bearbeitet: 10. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBackupServiceRolePolicyForRestores`

Version der Richtlinie

Richtlinienversion: v25 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:PutItem",
        "dynamodb:GetItem",
        "dynamodb:DeleteItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "DynamoDBBackupResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:RestoreTableFromBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*/backup/*"
    },
    {
      "Sid" : "EBSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonFSx" : "ManagedByAmazonFSx"
        }
      }
    },
    {
      "Sid" : "StorageGatewayVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DeleteVolume",
```

```
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:AddTagsToResource"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
      "Sid" : "StorageGatewayGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Sid" : "StorageGatewayListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:ListVolumes"
      ],
      "Resource" : "arn:aws:storagegateway:*:*:*"
    },
    {
      "Sid" : "RDSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:DeleteDBCluster",
        "rds:RestoreDBInstanceToPointInTime",
        "rds:DescribeDBClusterSnapshots",
        "rds:RestoreDBClusterToPointInTime",
        "rds:CreateTenantDatabase",
        "rds:DeleteTenantDatabase"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:TagResource"
      ],
      "Resource" : "arn:aws:elasticfilesystem:*:*:file-system/*"
    },
    {
      "Sid" : "KMSDescribePermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "*"
    },
    {
      "Sid" : "DSQLResourcePermissionsForRestore",
      "Effect" : "Allow",
      "Action" : [
        "dsql:StartRestoreJob",
        "dsql:GetRestoreJob",
        "dsql:StopRestoreJob",
        "dsql:TagResource",
        "dsql:CreateCluster",
        "dsql:PutMultiRegionProperties",
        "dsql:PutWitnessRegion",
        "dsql:UpdateCluster",
        "dsql:AddPeerCluster",
        "dsql:RemovePeerCluster",
        "dsql:GetCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "dynamodb.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "elasticfilesystem.*.amazonaws.com",
            "rds.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "dsql.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "KMSCreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "EBSSnapshotBlockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ebs:CompleteSnapshot",
        "ebs:StartSnapshot",
        "ebs:PutSnapshotBlock"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
```

```
      "Sid" : "RDSResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Sid" : "EC2DeleteAndRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:RestoreSnapshotTier"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "EC2CreateTagsScopedPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "EC2RunInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TerminateInstancesPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "EC2CreateTagsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateVolume"
          ]
        }
      }
    },
    {
      "Sid" : "FsxPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Sid" : "FsxTagPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "fsx:DescribeFileSystems",
        "fsx:TagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Sid" : "FsxBackupPermissions",
      "Effect" : "Allow",
      "Action" : "fsx:DescribeBackups",
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Sid" : "FsxDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:file-system/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "FsxDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeVolumes"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*"
    },
    {
      "Sid" : "FsxVolumeTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:volume/*"
      ],
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:backup:source-resource"
          ]
        }
      }
    },
    {
      "Sid" : "FsxBackupTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
      ],
      "Resource" : [
        "arn:aws:fsx:*:*:storage-virtual-machine/*",
        "arn:aws:fsx:*:*:backup/*",
        "arn:aws:fsx:*:*:volume/*"
      ]
    },
    {
      "Sid" : "FsxVolumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "fsx:DeleteVolume",
        "fsx:UntagResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/aws:backup:source-resource" : "false"
        }
      }
    },
    {
      "Sid" : "DSPermissions",
      "Effect" : "Allow",
      "Action" : "ds:DescribeDirectories",
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "dynamodb:RestoreTableFromAwsBackup"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Sid" : "GatewayRestorePermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup-gateway:Restore"
      ],
      "Resource" : "arn:aws:backup-gateway:*:*:hypervisor/*"
    },
    {
      "Sid" : "CloudformationChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:*/*/*"
    },
    {
      "Sid" : "RedshiftClusterSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:RestoreFromClusterSnapshot",
        "redshift:RestoreTableFromClusterSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:snapshot:*/*",
        "arn:aws:redshift:*:*:cluster:*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeClusters"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:cluster:*"
      ]
```

```
    },
    {
      "Sid" : "RedshiftTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeTableRestoreStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessSnapshotPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:RestoreTableFromSnapshot"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessNamespacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*"
      ]
    },
    {
      "Sid" : "RedshiftServerlessTablePermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetTableRestoreStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TimestreamResourcePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "timestream:StartAwsRestoreJob",
        "timestream:GetAwsRestoreStatus",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "timestream:ListDatabases",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase"
      ],
      "Resource" : [
        "arn:aws:timestream:*:*:database/*"
      ]
    },
    {
      "Sid" : "TimestreamEndpointPermissions",
      "Effect" : "Allow",
      "Action" : [
        "timestream:DescribeEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EKSClusterRestore",
      "Effect" : "Allow",
      "Action" : [
        "eks:CreateCluster",
        "eks:DescribeCluster",
        "eks:CreateAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:AssociateAccessPolicy",
        "eks:ListAssociatedAccessPolicies",
        "eks:CreateAddon",
        "eks:DescribeAddon",
        "eks:CreateNodegroup",
        "eks:DescribeNodegroup",
        "eks:CreateFargateProfile",
        "eks:DescribeFargateProfile",
        "eks:CreatePodIdentityAssociation",
        "eks:DescribePodIdentityAssociation",
        "eks:TagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:eks:*:*:access-entry/*",
        "arn:aws:eks:*:*:addon/*",
        "arn:aws:eks:*:*:cluster/*",
        "arn:aws:eks:*:*:fargateprofile/*",
        "arn:aws:eks:*:*:nodegroup/*",
        "arn:aws:eks:*:*:podidentityassociation/*"
      ]
    },
    {
      "Sid" : "AssociateRestoreAccessPolicy",
      "Effect" : "Allow",
      "Action" : [
        "eks:AssociateAccessPolicy",
        "eks:DisassociateAccessPolicy"
      ],
      "Resource" : "arn:aws:eks:*:*:access-entry/*",
      "Condition" : {
        "StringEquals" : {
          "eks:policyArn" : "arn:aws:eks::aws:cluster-access-policy/
AWSBackupFullAccessPolicyForRestore",
          "eks:accessScope" : "cluster"
        }
      }
    },
    {
      "Sid" : "CreateClusterIAMPerms",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "eks.amazonaws.com",
            "ec2.amazonaws.com",
            "pods.eks.amazonaws.com",
            "backup.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateEKSNodeGroupPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets",
        "ec2:RunInstances",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EKSNodeGroupTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "BackupRestoreJobManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "backup:StartRestoreJob",
        "backup:ListRestoreJobs",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:DescribeRestoreJob"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForS3Backup

Beschreibung: Richtlinie mit den für AWS Backup erforderlichen Berechtigungen zum Sichern von Daten in einem beliebigen S3-Bucket. Dazu gehören der Lesezugriff auf alle S3-Objekte und der Entschlüsselungszugriff für alle KMS-Schlüssel.

`AWSBackupServiceRolePolicyForS3Backup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForS3Backup` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2022, 17:40 UTC
- Bearbeitete Zeit: 17. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Backup`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchGetMetricDataPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "EventBridgePermissionsForAwsBackupManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AwsBackupManagedRule*"
      ]
    },
    {
      "Sid" : "EventBridgeListRulesPermissions",
      "Effect" : "Allow",
      "Action" : "events:ListRules",
      "Resource" : "*"
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:GetInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutInventoryConfiguration",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3ObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/*"
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListAllMyBuckets",
      "Resource" : "*"
    },
    {
      "Sid" : "RecoveryPointTaggingPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "backup:TagResource"
      ],
      "Resource" : "arn:aws:backup:*:*:recovery-point:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForS3Restore

Beschreibung: Richtlinie mit Berechtigungen, die AWS Backup benötigt, um ein S3-Backup in einem Bucket wiederherzustellen. Dazu gehören read/write Berechtigungen für alle S3-Buckets sowie Berechtigungen DescribeKey für GenerateDataKey und für alle KMS-Schlüssel.

`AWSBackupServiceRolePolicyForS3Restore`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForS3Restore` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2022, 17:39 UTC
- Bearbeitete Zeit: 7. Februar 2023, 00:06 UTC

- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForS3Restore`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning",
        "s3:PutBucketOwnershipControls",
        "s3:GetBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
```

```
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBackupServiceRolePolicyForScans

Beschreibung: Bietet AWS Backup-Berechtigungen zur Durchführung von Malware-Scans auf Ihren AWS Backup-Wiederherstellungspunkten

`AWSBackupServiceRolePolicyForScans`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBackupServiceRolePolicyForScans` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2025, 03:34 UTC
- Bearbeitete Zeit: 20. November 2025, 03:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBackupServiceRolePolicyForScans`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GuardDutyMalwareScanPermissions",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:StartMalwareScan",
        "guardduty:GetMalwareScan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMPassPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "malware-protection.guardduty.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ReadAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Batch-Ressourcen.

`AWSBatchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBatchFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2016, 19:35 UTC

- Bearbeitete Zeit: 24. Oktober 2022, 16:09 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBatchFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:*",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ecs:DescribeClusters",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:ListClusters",
        "logs:Describe*",
        "logs:Get*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/service-role/AWSBatchServiceRole",
        "arn:aws:iam::*:role/ecsInstanceRole",
        "arn:aws:iam::*:instance-profile/ecsInstanceRole",
        "arn:aws:iam::*:role/iaws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-role",
        "arn:aws:iam::*:role/AWSBatchJobRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*Batch*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "batch.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchServiceEventTargetRole

Beschreibung: Richtlinie zur Aktivierung von CloudWatch Event Target für die Einreichung von AWS Batch-Jobs

`AWSBatchServiceEventTargetRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBatchServiceEventTargetRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Februar 2018, 22:31 UTC
- Bearbeitete Zeit: 28. Februar 2018, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceEventTargetRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "batch:SubmitJob"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchServiceRole

Beschreibung: Richtlinie für die AWS Batch-Servicerolle, die den Zugriff auf verwandte Dienste wie Autoscaling EC2, EC2 Container-Service und Cloudwatch Logs ermöglicht.

`AWSBatchServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBatchServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2016, 19:36 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSBatchServiceRole`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:TerminateInstances",
        "ec2:RunInstances",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
```

```
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListAccountSettings",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:RegisterTaskDefinition",
        "ecs:DeregisterTaskDefinition",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:UpdateContainerAgent",
        "ecs:DeregisterContainerInstance",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : "ecs:TagResource",
      "Resource" : [
        "arn:aws:ecs:*:*:task/*_Batch_*"
      ]
    },
    {
```

```
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBatchServiceRolePolicyForSageMaker

Beschreibung: Ermöglicht AWS Batch den Zugriff auf die Warteschlange und Verwaltung von SageMaker Amazon-Workloads

`AWSBatchServiceRolePolicyForSageMaker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Juli 2025, 21:37 UTC
- Bearbeitete Zeit: 15. Juli 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBatchServiceRolePolicyForSageMaker`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-plan/*",
        "arn:aws:sagemaker:*:*:reserved-capacity/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:training-job/AWSBatch*",
      "Condition" : {
        "StringEquals" : {
```

```
          "sagemaker:TaggingAction" : "CreateTrainingJob"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTrainingJobs",
        "sagemaker:Search"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBCMDataExportsServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle, die Abrechnungs- und Kostenmanagement-Datenexporten Zugriff auf AWS Servicedaten ermöglicht, um die Daten im Namen eines Kunden an einen Zielort wie Amazon S3 zu exportieren.

`AWSBCMDataExportsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juni 2024, 17:40 UTC
- Bearbeitete Zeit: 10. Juni 2024, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBCMDataExportsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationRecommendationAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingConductorFullAccess

Beschreibung: Verwenden Sie die AWSBilling ConductorFullAccess verwaltete Richtlinie, um vollständigen Zugriff auf die AWS Billing Conductor (ABC-) Konsole und zu ermöglichen APIs. Diese Richtlinie ermöglicht es Benutzern, ABC-Ressourcen aufzulisten, zu erstellen und zu löschen.

`AWSBillingConductorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBillingConductorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 27. November 2025, 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:*",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:DescribeResponsibilityTransfer",
        "organizations:ListInboundResponsibilityTransfers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingConductorReadOnlyAccess

Beschreibung: Verwenden Sie die AWSBilling ConductorReadOnlyAccess verwaltete Richtlinie, um nur Lesezugriff auf die AWS Billing Conductor (ABC-) Konsole und zuzulassen APIs. Diese Richtlinie gewährt die Berechtigung zum Anzeigen und Auflisten aller ABC-Ressourcen. Sie beinhaltet nicht die Möglichkeit, Ressourcen zu erstellen oder zu löschen.

`AWSBillingConductorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBillingConductorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. April 2022, 18:02 UTC
- Bearbeitete Zeit: 18. September 2025, 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingConductorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billingconductor:List*",
        "billingconductor:GetBillingGroupCostReport",
        "organizations:ListAccounts",
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:DescribeAccount"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingReadOnlyAccess

Beschreibung: Ermöglicht Benutzern, Rechnungen in der Abrechnungskonsole einzusehen.

`AWSBillingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBillingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. August 2020, 20:08 UTC
- Bearbeitete Zeit: 18. November 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBillingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetCredits",
        "billing:GetContractInformation",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "budgets:ViewBudget",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:ListCostAllocationTags",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostComparisonDrivers",
        "consolidatedbilling:ListLinkedAccounts",
        "consolidatedbilling:GetAccountBillingRole",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
```

```
        "cur:DescribeReportDefinitions",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountPlanState",
        "freetier:GetAccountActivity",
        "freetier:ListAccountActivities",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "sustainability:GetCarbonFootprintSummary",
        "tax:GetTaxRegistrationDocument",
        "tax:GetTaxInheritance",
        "tax:ListTaxRegistrations"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBillingServiceRolePolicy

Beschreibung: Ermöglicht dem Abrechnungsservice, den Zugriff auf Abrechnungsansichtsdaten für abgeleitete Abrechnungsansichten zu validieren

`AWSBillingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. September 2025, 16:19 UTC
- Bearbeitete Zeit: 11. September 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBillingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "billing:GetBillingViewData"
      ],
      "Resource" : "arn:aws:billing::*:billingview/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Steuerung von AWS Ressourcen. Zum Beispiel, um RDS-Instances zu starten und zu stoppen EC2 , indem AWS Systems Manager (SSM) -Skripts ausgeführt werden.

`AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Mai 2022, 19:03 UTC
- Bearbeitete Zeit: 25. Mai 2022, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActions_RolePolicyForResourceAdministrationWithSSM`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ssm.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-StartEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopEC2Instance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StartRdsInstance:*",
        "arn:aws:ssm:*:*:automation-definition/AWS-StopRdsInstance:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsActionsWithAWSResourceControlAccess

Beschreibung: Bietet vollen Zugriff auf AWS Budgetaktionen, einschließlich der Verwendung von Budgetaktionen zur Steuerung des Status laufender AWS Ressourcen über AWS-Managementkonsole

`AWSBudgetsActionsWithAWSResourceControlAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBudgetsActionsWithAWSResourceControlAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 15. Oktober 2020, 17:19 Uhr UTC
- Zeit bearbeitet: 15. Oktober 2020, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsActionsWithAWSResourceControlAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "budgets:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "budgets.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ModifyBilling",
        "ec2:DescribeInstances",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListPolicies",
        "organizations:ListRoots",
        "rds:DescribeDBInstances",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBudgetsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Budget-Konsole über die AWS-Managementkonsole.

`AWSBudgetsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBudgetsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Oktober 2020, 17:18 Uhr UTC
- Bearbeitete Zeit: 17. Juni 2024, 17:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBudgetsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSBudgetsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-portal:ViewBilling",
        "budgets:ViewBudget",
        "budgets:Describe*",
        "budgets:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustFullAccess

Beschreibung: Diese IAM-Richtlinie gewährt Benutzern vollen Zugriff auf die Konsole AWS BugBust

`AWSBugBustFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBugBustFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2021, 07:03 UTC
- Bearbeitete Zeit: 22. Juli 2021, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustSLRCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/bugbust.amazonaws.com/
AWSServiceRoleForBugBust",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "bugbust.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustPlayerAccess

Beschreibung: Diese IAM-Richtlinie gewährt Benutzern Zugriff auf die Teilnahme AWS BugBust an Veranstaltungen

`AWSBugBustPlayerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSBugBustPlayerAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2021, 07:15 Uhr UTC
- Bearbeitete Zeit: 24. Juni 2021, 07:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSBugBustPlayerAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeGuruReviewerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeGuruProfilerPermission",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-profiler:DescribeProfilingGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSBugBustPlayerAccess",
      "Effect" : "Allow",
      "Action" : [
        "bugbust:ListBugs",
        "bugbust:ListProfilingGroups",
        "bugbust:JoinEvent",
        "bugbust:GetEvent",
        "bugbust:ListEvents",
        "bugbust:GetJoinEventStatus",
        "bugbust:ListEventScores",
        "bugbust:ListEventParticipants",
        "bugbust:UpdateWorkItem",
        "bugbust:ListPullRequests"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSBugBustServiceRolePolicy

Beschreibung: Erteilt die Erlaubnis AWS BugBust , in Ihrem Namen auf Ressourcen zuzugreifen

`AWSBugBustServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Juni 2021, 06:59 UTC
- Bearbeitete Zeit: 24. Juni 2021, 06:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSBugBustServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:ListRecommendations",
        "codeguru-reviewer:UntagResource",
        "codeguru-reviewer:DescribeCodeReview"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/bugbust" : "enabled"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Certificate Manager (ACM)

`AWSCertificateManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2016, 17:02 UTC
- Bearbeitete Zeit: 17. August 2020, 22:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "acm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/acm.amazonaws.com/
AWSServiceRoleForCertificateManager*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAAuditor

Beschreibung: Bietet Auditor-Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAAuditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerPrivateCAAuditor` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:51 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAAuditor`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerPrivateCAFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:54 UTC
- Bearbeitete Zeit: 23. Oktober 2018, 16:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAPrivilegedUser

Beschreibung: Bietet privilegierten Zertifikatsbenutzern Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAPrivilegedUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerPrivateCAPrivilegedUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Juni 2019, 17:43 UTC
- Zeit bearbeitet: 22. Januar 2025, 19:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAPrivilegedUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerPrivateCAReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:57 UTC
- Bearbeitete Zeit: 17. August 2020, 22:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerPrivateCAUser

Beschreibung: Bietet Zertifikatsbenutzerzugriff auf AWS Certificate Manager Private Certificate Authority

`AWSCertificateManagerPrivateCAUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerPrivateCAUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Oktober 2018, 16:53 UTC
- Zeit bearbeitet: 22. Januar 2025, 15:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerPrivateCAUser`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCertificateManagerReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Certificate Manager (ACM).

`AWSCertificateManagerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCertificateManagerReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Januar 2016, 17:07 UTC
- Bearbeitete Zeit: 15. März 2021, 16:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCertificateManagerReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm:DescribeCertificate",
      "acm:ListCertificates",
      "acm:GetCertificate",
      "acm:ListTagsForCertificate",
      "acm:GetAccountConfiguration"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSChatbotServiceLinkedRolePolicy

Beschreibung: Die vom AWS Chatbot verwendete serviceverknüpfte Rolle.

`AWSChatbotServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2019, 16:39 Uhr UTC
- Bearbeitete Zeit: 18. November 2019, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSChatbotServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Unsubscribe",
        "sns:Subscribe",
        "sns:ListSubscriptions"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/chatbot/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf AWS Clean Rooms-Ressourcen und den Zugriff auf verwandte Ressourcen AWS-Services.

`AWSCleanRoomsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCleanRoomsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:10 UTC
- Bearbeitete Zeit: 21. März 2024, 15:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ConsolePickQueryResultsBucketListAll",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SetQueryResultsBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "WriteQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleDisplayQueryResults",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::cleanrooms-queryresults*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
```

```
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsFullAccessNoQuerying

Beschreibung: Ermöglicht vollen Zugriff auf AWS Clean Rooms-Ressourcen mit Ausnahme von Abfragen in einer Kollaboration und Zugriff auf verwandte AWS-Services Ressourcen.

`AWSCleanRoomsFullAccessNoQuerying`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCleanRoomsFullAccessNoQuerying` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:12 UTC
- Bearbeitete Zeit: 13. August 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsFullAccessNoQuerying`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:CreateAnalysisTemplate",
        "cleanrooms:CreateCollaboration",
        "cleanrooms:CreateConfiguredTable",
        "cleanrooms:CreateConfiguredTableAnalysisRule",
        "cleanrooms:CreateConfiguredTableAssociation",
        "cleanrooms:CreateMembership",
        "cleanrooms:DeleteAnalysisTemplate",
```

```
        "cleanrooms:DeleteCollaboration",
        "cleanrooms:DeleteConfiguredTable",
        "cleanrooms:DeleteConfiguredTableAnalysisRule",
        "cleanrooms:DeleteConfiguredTableAssociation",
        "cleanrooms:DeleteMember",
        "cleanrooms:DeleteMembership",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:UpdateAnalysisTemplate",
        "cleanrooms:UpdateCollaboration",
        "cleanrooms:UpdateConfiguredTable",
        "cleanrooms:UpdateConfiguredTableReference",
        "cleanrooms:UpdateConfiguredTableAllowedColumns",
        "cleanrooms:UpdateConfiguredTableAnalysisRule",
        "cleanrooms:UpdateConfiguredTableAssociation",
        "cleanrooms:UpdateMembership",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:UntagResource",
        "cleanrooms:TagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsNoQuerying",
      "Effect" : "Deny",
      "Action" : [
        "cleanrooms:StartProtectedQuery",
```

```
        "cleanrooms:UpdateProtectedQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/*cleanrooms*"
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanrooms*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EstablishLogDeliveries",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsDescribe",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsCreate",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SetupLogGroupsResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cleanrooms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
```

```
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf AWS Clean Rooms ML-Ressourcen und den Zugriff auf verwandte Ressourcen AWS-Services.

`AWSCleanRoomsMLFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCleanRoomsMLFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 21:02 UTC
- Bearbeitete Zeit: 10. Januar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsMLFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/cleanrooms-ml*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cleanrooms-ml.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:BatchGetSchema",
```

```
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CollaborationMembershipCheck",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:ListMembers"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cleanrooms-ml.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AssociateModels",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:CreateConfiguredAudienceModelAssociation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAssociations",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:TagResource"
```

```
      ],
      "Resource" : "arn:aws:cleanrooms:*:*:membership/*/
configuredaudiencemodelassociation/*"
    },
    {
      "Sid" : "ListRolesToPickServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetRoleAndListRolePoliciesToInspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cleanrooms-ml*",
        "arn:aws:iam::*:role/role/cleanrooms-ml*"
      ]
    },
    {
      "Sid" : "ListPoliciesToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetPolicyToInspectServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : "arn:aws:iam::*:policy/*cleanroomsml*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
```

```
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickOutputBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsolePickS3Location",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*cleanrooms-ml*"
    },
    {
      "Sid" : "ConsoleDescribeECRRepositories",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:ListImages"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsMLReadOnlyAccess

Beschreibung: Ermöglicht den schreibgeschützten Zugriff auf AWS Clean Rooms ML-Ressourcen und den schreibgeschützten Zugriff auf zugehörige Clean Rooms-Ressourcen AWS

`AWSCleanRoomsMLReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSCleanRoomsMLReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2023, 20:55 UTC
- Bearbeitete Zeit: 10. Januar 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsMLReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsConsoleNavigation",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CleanRoomsMLRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms-ml:Get*",
        "cleanrooms-ml:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassCleanRoomsResources",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cleanrooms:PassMembership",
        "cleanrooms:PassCollaboration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsReadOnlyAccess

Beschreibung: Ermöglicht den schreibgeschützten Zugriff auf AWS Clean Rooms-Ressourcen und den schreibgeschützten Zugriff auf zugehörige AWS Glue- und Amazon Logs-Ressourcen. CloudWatch

`AWSCleanRoomsReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSCleanRoomsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Januar 2023, 16:10 UTC
- Bearbeitete Zeit: 12. Januar 2023, 16:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCleanRoomsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CleanRoomsRead",
      "Effect" : "Allow",
      "Action" : [
        "cleanrooms:BatchGet*",
        "cleanrooms:Get*",
        "cleanrooms:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleDisplayTables",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetSchema",
        "glue:GetSchemaVersion",
        "glue:BatchGetPartition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleLogSummaryQueryLogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:StartQuery"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cleanrooms*"
    },
    {
      "Sid" : "ConsoleLogSummaryObtainLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:GetQueryResults"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCleanRoomsServiceRolePolicy

Beschreibung: Erlauben AWS Sie Clean Rooms, auf andere AWS Dienste zuzugreifen, z. CloudWatch APIs B. in Ihrem Namen.

`AWSCleanRoomsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 15. Dezember 2025, 17:49 UTC
- Bearbeitete Zeit: 15. Dezember 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCleanRoomsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Clean Rooms"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9Administrator

Beschreibung: Bietet Administratorzugriff auf AWS Cloud9.

`AWSCloud9Administrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloud9Administrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:17 UTC
- Bearbeitete Zeit: 25. September 2025, 11:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9Administrator`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:*",
        "iam:GetUser",
```

```
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9EnvironmentMember

Beschreibung: Bietet die Möglichkeit, in gemeinsam genutzte AWS Cloud9-Entwicklungsumgebungen eingeladen zu werden.

`AWSCloud9EnvironmentMember`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloud9EnvironmentMember` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:18 Uhr UTC
- Zeit bearbeitet: 25. September 2025, 11:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9EnvironmentMember`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserSettings",
        "cloud9:UpdateUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9ServiceRolePolicy

Beschreibung: Service Linked Role Policy für AWS Cloud9

`AWSCloud9ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2017, 13:44 Uhr UTC
- Bearbeitete Zeit: 17. Januar 2022, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloud9ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-cloud9-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/Name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-name" : "aws-cloud9-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : [
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/cloud9/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSCloud9SSMAccessRole"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9SSMInstanceProfile

Beschreibung: Diese Richtlinie wird verwendet, um einer Rolle eine Rolle zuzuweisen InstanceProfile , sodass Cloud9 den SSM Session Manager verwenden kann, um eine Verbindung zur Instanz herzustellen

`AWSCloud9SSMInstanceProfile`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloud9SSMInstanceProfile` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Mai 2020, 11:40 UTC
- Bearbeitete Zeit: 14. Mai 2020, 11:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9SSMInstanceProfile`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloud9User

Beschreibung: Erlaubt die Erlaubnis, AWS Cloud9-Entwicklungsumgebungen zu erstellen und eigene Umgebungen zu verwalten.

`AWSCloud9User`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloud9User` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2017, 16:16 UTC
- Bearbeitete Zeit: 25. September 2025, 11:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloud9User`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:UpdateUserSettings",
        "cloud9:GetUserSettings",
        "cloud9:GetMigrationExperiences",
        "iam:GetUser",
        "iam:ListUsers",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:CreateEnvironmentEC2",
```

```
        "cloud9:CreateEnvironmentSSH"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:OwnerArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:GetUserPublicKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloud9:DescribeEnvironmentMemberships"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "cloud9:UserArn" : "true",
          "cloud9:EnvironmentId" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ssm:resourceTag/aws:cloud9:environment" : "*"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:session/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFormationFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CloudFormation.

`AWSCloudFormationFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudFormationFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2019, 21:50 Uhr UTC
- Bearbeitete Zeit: 26. Juli 2019, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFormationReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf AWS CloudFormation über die AWS-Managementkonsole.

`AWSCloudFormationReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudFormationReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 13. November 2019, 17:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudFormationReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:EstimateTemplateCost",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudformation:Detect*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFrontLogger

Beschreibung: Gewährt CloudFront Logger Schreibberechtigungen für CloudWatch Logs.

`AWSCloudFrontLogger`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2018, 20:15 Uhr UTC
- Bearbeitete Zeit: 22. November 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontLogger`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/cloudfront/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudFrontVPCOriginServiceRolePolicy

Beschreibung: Ermöglicht CloudFront die Verwaltung von EC2 Elastic Network Interfaces und Security Groups in Ihrem Namen.

`AWSCloudFrontVPCOriginServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2024, 17:45 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudFrontVPCOriginServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:network-interface/*"
    },
    {
      "Sid" : "EC2Action2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "EC2Action5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws.cloudfront.vpcorigin" : "enabled"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2Action7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws.cloudfront.vpcorigin" : "enabled",
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "CreateSecurityGroup"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMFullAccess

Beschreibung: Bietet vollen Zugriff auf alle CloudHSM-Ressourcen.

`AWSCloudHSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudHSMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudhsm:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle CloudHSM-Ressourcen.

`AWSCloudHSMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudHSMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudHSMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Get*",
        "cloudhsm:List*",
        "cloudhsm:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudHSMRole

Beschreibung: Standardrichtlinie für die AWS CloudHSM-Servicerolle.

`AWSCloudHSMRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudHSMRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCloudHSMRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapDiscoverInstanceAccess

Beschreibung: Bietet Zugriff auf die AWS Cloud Map Discovery API.

`AWSCloudMapDiscoverInstanceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudMapDiscoverInstanceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:02 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Cloud Kartenaktionen.

`AWSCloudMapFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudMapFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 23:57 UTC
- Bearbeitete Zeit: 29. Juli 2020, 19:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "servicediscovery:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle AWS Cloud Map-Aktionen.

`AWSCloudMapReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudMapReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 23:45 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision"
      ],
      "Resource" : [
```

```
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudMapRegisterInstanceAccess

Beschreibung: Bietet Zugriff auf Registrantenebene auf AWS Cloud Map-Aktionen.

`AWSCloudMapRegisterInstanceAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudMapRegisterInstanceAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 00:04 Uhr UTC
- Bearbeitete Zeit: 20. September 2023, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudMapRegisterInstanceAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListHostedZonesByName",
        "route53:ChangeResourceRecordSets",
        "route53:CreateHealthCheck",
        "route53:GetHealthCheck",
        "route53:DeleteHealthCheck",
        "route53:UpdateHealthCheck",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicediscovery:RegisterInstance",
        "servicediscovery:DeregisterInstance",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudShellFullAccess

Beschreibung: Ermöglicht die Nutzung AWS CloudShell mit allen Funktionen

`AWSCloudShellFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudShellFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 18:07 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudShellFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudshell:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudTrail_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CloudTrail.

`AWSCloudTrail_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudTrail_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2020, 23:41 UTC
- Bearbeitete Zeit: 22. Februar 2021, 19:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:GetTopicAttributes"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudtrail:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateKey",
        "kms:CreateAlias",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudTrail_ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CloudTrail.

`AWSCloudTrail_ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCloudTrail_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Juni 2022, 17:19 UTC
- Bearbeitete Zeit: 14. Juni 2022, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCloudTrail_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:Get*",
        "cloudtrail:Describe*",
        "cloudtrail:List*",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy

Beschreibung: Diese Richtlinie wird von der mit dem Dienst verknüpften Rolle mit dem Namen AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents verwendet. CloudWatch verwendet diese dienstbezogene Rolle, um AWS System Manager Incident Manager-Aktionen auszuführen, wenn ein CloudWatch Alarm in den ALARM-Status wechselt. Diese Richtlinie erteilt die Erlaubnis, Incidents in Ihrem Namen zu starten.

`AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. April 2021, 13:30 Uhr UTC
- Bearbeitete Zeit: 27. April 2021, 13:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-incidents:StartIncident",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeArtifactAdminAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeArtifact über die AWS-Managementkonsole.

`AWSCodeArtifactAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeArtifactAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Juni 2020, 23:53 UTC
- Bearbeitete Zeit: 16. Juni 2020, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeArtifactReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeArtifact über die AWS-Managementkonsole.

`AWSCodeArtifactReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeArtifactReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2020, 21:23 Uhr UTC
- Bearbeitete Zeit: 25. Juni 2020, 21:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeArtifactReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codeartifact:Describe*",
```

```
        "codeartifact:Get*",
        "codeartifact:List*",
        "codeartifact:ReadFromRepository"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:GetServiceBearerToken",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "sts:AWSServiceName" : "codeartifact.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildAdminAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeBuild über die AWS-Managementkonsole. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren, und fügen Sie IAMFull Access hinzu, um die Servicerolle für zu erstellen und zu verwalten. CodeBuild

`AWSCodeBuildAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeBuildAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:04 UTC
- Bearbeitete Zeit: 16. Dezember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess`

Version der Richtlinie

Richtlinienversion: v15 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "elasticfilesystem:DescribeFileSystems",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
```

```
        "events:EnableRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CWLDeleteLogGroupAccess",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/codebuild/*:log-stream:*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:CreateConnection",
        "codestar-connections:DeleteConnection",
        "codestar-connections:UpdateConnectionInstallation",
```

```
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:ListTagsForResource",
        "codestar-connections:GetConnection",
        "codestar-connections:GetIndividualAccessToken",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:PassConnection",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildDeveloperAccess

Beschreibung: Ermöglicht den Zugriff auf AWS CodeBuild über AWS-Managementkonsole, ermöglicht jedoch keine CodeBuild Projektverwaltung. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren.

`AWSCodeBuildDeveloperAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeBuildDeveloperAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:02 UTC
- Bearbeitete Zeit: 16. Dezember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildDeveloperAccess`

Version der Richtlinie

Richtlinienversion: v16 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:StartBuildBatch",
        "codebuild:StopBuildBatch",
        "codebuild:RetryBuild",
```

```
        "codebuild:RetryBuildBatch",
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codebuild:List*",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameterWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/CodeBuild/*"
    },
    {
      "Sid" : "SSMStartSessionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
```

```
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeBuildReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeBuild über die AWS-Managementkonsole. Fügen Sie außerdem AmazonS3 hinzuReadOnlyAccess , um Zugriff auf Download-Build-Artefakte zu gewähren.

`AWSCodeBuildReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeBuildReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 19:03 UTC
- Bearbeitete Zeit: 16. Dezember 2024, 19:52 UTC

- ARN: `arn:aws:iam::aws:policy/AWSCodeBuildReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSServicesAccess",
      "Action" : [
        "codebuild:BatchGet*",
        "codebuild:GetResourcePolicy",
        "codebuild:List*",
        "codebuild:DescribeTestCases",
        "codebuild:DescribeCodeCoverages",
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "cloudwatch:GetMetricStatistics",
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "events:ListRuleNamesByTarget",
        "logs:GetLogEvents"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
```

```
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codebuild:*:*:project/*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeCommit über die AWS-Managementkonsole.

`AWSCodeCommitFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeCommitFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:02 UTC
- Bearbeitete Zeit: 10. Januar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
```

```
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitPowerUser

Beschreibung: Bietet vollen Zugriff auf AWS CodeCommit Repositorys, erlaubt aber nicht das Löschen von Repositorys.

`AWSCodeCommitPowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeCommitPowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:06 UTC
- Bearbeitete Zeit: 10. Januar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitPowerUser`

Version der Richtlinie

Richtlinienversion: v16 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codecommit:AssociateApprovalRuleTemplateWithRepository",
        "codecommit:BatchAssociateApprovalRuleTemplateWithRepositories",
        "codecommit:BatchDisassociateApprovalRuleTemplateFromRepositories",
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Create*",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:Describe*",
        "codecommit:DisassociateApprovalRuleTemplateFromRepository",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:Merge*",
        "codecommit:OverridePullRequestApprovalRules",
        "codecommit:Put*",
        "codecommit:Post*",
        "codecommit:TagResource",
        "codecommit:Test*",
        "codecommit:UntagResource",
        "codecommit:Update*",
        "codecommit:GitPull",
        "codecommit:GitPush"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "events:DeleteRule",
        "events:DescribeRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:codecommit*"
    },
    {
      "Sid" : "SNSTopicAndSubscriptionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAccessKeys",
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMUserSSHKeys",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "IAMSelfManageServiceSpecificCredentials",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:AssociateRepository",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DisassociateRepository",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerSLRCreation",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/codeguru-
reviewer.amazonaws.com/AWSServiceRoleForAmazonCodeGuruReviewer",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "codeguru-reviewer.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchEventsManagedRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "codeguru-reviewer.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeCommitReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodeCommit über die AWS-Managementkonsole.

`AWSCodeCommitReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeCommitReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:05 UTC
- Bearbeitete Zeit: 10. Januar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeCommitReadOnly`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "codecommit:BatchGet*",
        "codecommit:BatchDescribe*",
        "codecommit:Describe*",
        "codecommit:EvaluatePullRequestApprovalRules",
        "codecommit:Get*",
        "codecommit:List*",
        "codecommit:GitPull"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchEventsCodeCommitRulesReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/codecommit*"
    },
    {
      "Sid" : "SNSSubscriptionAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics",
        "sns:ListSubscriptionsByTopic",
        "sns:GetTopicAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListUsers"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyConsoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListSSHPublicKeys",
        "iam:ListServiceSpecificCredentials",
        "iam:ListAccessKeys",
        "iam:GetSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    },
    {
      "Sid" : "CodeStarConnectionsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codecommit:*:*:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonCodeGuruReviewerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codeguru-reviewer:DescribeCodeReview",
        "codeguru-reviewer:ListCodeReviews"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployDeployerAccess

Beschreibung: Ermöglicht den Zugriff auf die Registrierung und Bereitstellung einer Revision.

`AWSCodeDeployDeployerAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployDeployerAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:18 Uhr UTC

- Bearbeitete Zeit: 16. Dezember 2024, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployDeployerAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:CreateDeployment",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codedeploy:RegisterApplicationRevision"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployFullAccess

Beschreibung: Bietet vollen Zugriff auf CodeDeploy Ressourcen.

`AWSCodeDeployFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:13 Uhr UTC
- Bearbeitete Zeit: 16. Dezember 2024, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "codedeploy:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
"arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "SNSTopicListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CodeDeploy Ressourcen.

`AWSCodeDeployReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Mai 2015, 18:21 Uhr UTC
- Bearbeitete Zeit: 16. Dezember 2024, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarNotificationsPowerUserAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "codestar-notifications:NotificationsForResource" :
 "arn:aws:codedeploy:*:*:application:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsListAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRole

Beschreibung: Bietet CodeDeploy Servicezugriff, um Tags zu erweitern und in Ihrem Namen mit Auto Scaling zu interagieren.

`AWSCodeDeployRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Mai 2015, 18:05 Uhr UTC
- Bearbeitete Zeit: 16. August 2023, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRole`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:DeleteLifecycleHook",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:PutLifecycleHook",
        "autoscaling:RecordLifecycleActionHeartbeat",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:SuspendProcesses",
        "autoscaling:ResumeProcesses",
        "autoscaling:AttachLoadBalancers",
        "autoscaling:AttachLoadBalancerTargetGroups",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutWarmPool",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DeleteAutoScalingGroup",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:TerminateInstances",
        "tag:GetResources",
        "sns:Publish",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:PutMetricAlarm",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForCloudFormation

Beschreibung: Bietet CodeDeploy Servicezugriff zum Aufrufen der Lambda-Funktion in Ihrem Namen, um die blue/green Bereitstellung durchzuführen. CloudFormation

`AWSCodeDeployRoleForCloudFormation`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRoleForCloudFormation` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2020, 17:12 Uhr UTC

- Bearbeitete Zeit: 19. Mai 2020, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForCloudFormation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForECS

Beschreibung: Bietet CodeDeploy serviceweiten Zugriff, sodass Sie eine blue/green ECS-Bereitstellung in Ihrem Namen durchführen können. Gewährt vollen Zugriff auf Support-Services, z. B. vollen Zugriff zum Lesen aller S3-Objekte, zum Aufrufen aller Lambda-Funktionen, zum Veröffentlichen zu allen SNS-Themen innerhalb des Kontos und zum Aktualisieren aller ECS-Services.

`AWSCodeDeployRoleForECS`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRoleForECS` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 20:40 UTC
- Bearbeitete Zeit: 23. September 2019, 22:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
```

```
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule",
        "lambda:InvokeFunction",
        "cloudwatch:DescribeAlarms",
        "sns:Publish",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForECSLimited

Beschreibung: Bietet eingeschränkten CodeDeploy Servicezugriff zur Durchführung einer blue/green ECS-Bereitstellung in Ihrem Namen.

`AWSCodeDeployRoleForECSLimited`dist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRoleForECSLimited` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 20:42 UTC
- Bearbeitete Zeit: 23. September 2019, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ecs:DescribeServices",
        "ecs:CreateTaskSet",
        "ecs:UpdateServicePrimaryTaskSet",
        "ecs:DeleteTaskSet",
        "cloudwatch:DescribeAlarms"
      ],
```

```
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeDeployTopic_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:ModifyRule"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/ecsTaskExecutionRole",
        "arn:aws:iam::*:role/ECSTaskExecution*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForLambda

Beschreibung: Bietet CodeDeploy Servicezugriff, um eine Lambda-Bereitstellung in Ihrem Namen durchzuführen.

`AWSCodeDeployRoleForLambda`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRoleForLambda` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 28. November 2017, 14:05 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambda`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig",
        "sns:Publish"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeDeployRoleForLambdaLimited

Beschreibung: Bietet eingeschränkten CodeDeploy Dienstzugriff zur Durchführung einer Lambda-Bereitstellung in Ihrem Namen.

`AWSCodeDeployRoleForLambdaLimited`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeDeployRoleForLambdaLimited` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. August 2020, 17:14 Uhr UTC
- Bearbeitete Zeit: 17. August 2020, 17:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeDeployRoleForLambdaLimited`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "lambda:UpdateAlias",
        "lambda:GetAlias",
        "lambda:GetProvisionedConcurrencyConfig"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/CodeDeploy/*",
      "Effect" : "Allow"
    },
```

```
    {
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ExistingObjectTag/UseWithCodeDeploy" : "true"
        }
      },
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:CodeDeployHook_*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipeline_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodePipeline über die AWS-Managementkonsole.

`AWSCodePipeline_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodePipeline_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. August 2020, 22:38 UTC
- Bearbeitete Zeit: 14. März 2024, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListChangeSets",
        "cloudtrail:DescribeTrails",
        "codebuild:BatchGetProjects",
        "codebuild:CreateProject",
        "codebuild:ListCuratedEnvironmentImages",
        "codebuild:ListProjects",
        "codecommit:ListBranches",
        "codecommit:GetReferences",
        "codecommit:ListRepositories",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:ListClusters",
        "ecs:ListServices",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "iam:ListRoles",
        "iam:GetRole",
        "lambda:ListFunctions",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:DescribeRule",
        "opsworks:DescribeApps",
        "opsworks:DescribeLayers",
        "opsworks:DescribeStacks",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListTargets",
        "codestar-notifications:ListTagsforResource",
        "codestar-notifications:ListEventTypes",
        "states:ListStateMachines"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Sid" : "CodePipelineAuthoringAccess"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetObjectVersion",
        "s3:CreateBucket",
        "s3:PutBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*",
      "Sid" : "CodePipelineArtifactsReadWriteAccess"
    },
    {
      "Action" : [
        "cloudtrail:PutEventSelectors",
```

```
        "cloudtrail:CreateTrail",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:StartLogging"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudtrail:*:*:trail/codepipeline-source-trail",
      "Sid" : "CodePipelineSourceTrailReadWriteAccess"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/cwe-role-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "events.amazonaws.com"
          ]
        }
      },
      "Sid" : "EventsIAMPassRole"
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "codepipeline.amazonaws.com"
          ]
        }
      },
      "Sid" : "CodePipelineIAMPassRole"
    },
    {
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
```

```
        "events:DeleteRule",
        "events:DisableRule",
        "events:RemoveTargets"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:events:*:*:rule/codepipeline-*"
      ],
      "Sid" : "CodePipelineEventsReadWriteAccess"
    },
    {
      "Sid" : "CodeStarNotificationsReadWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:CreateNotificationRule",
        "codestar-notifications:DescribeNotificationRule",
        "codestar-notifications:UpdateNotificationRule",
        "codestar-notifications:DeleteNotificationRule",
        "codestar-notifications:Subscribe",
        "codestar-notifications:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    },
    {
      "Sid" : "CodeStarNotificationsSNSTopicCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes"
      ],
      "Resource" : "arn:aws:sns:*:*:codestar-notifications*"
    },
    {
      "Sid" : "CodeStarNotificationsChatbotAccess",
      "Effect" : "Allow",
      "Action" : [
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:ListMicrosoftTeamsChannelConfigurations"
      ],
```

```
      "Resource" : "*"
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipeline_ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS CodePipeline über die AWS-Managementkonsole.

`AWSCodePipeline_ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodePipeline_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. August 2020, 22:25 Uhr UTC
- Bearbeitete Zeit: 3. August 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipeline_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListActionExecutions",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "codestar-notifications:ListNotificationRules",
        "codestar-notifications:ListEventTypes",
        "codestar-notifications:ListTargets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketPolicy"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:s3::*:codepipeline-*"
    },
    {
      "Sid" : "CodeStarNotificationsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "codestar-notifications:DescribeNotificationRule"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "codestar-notifications:NotificationsForResource" : "arn:aws:codepipeline:*"
        }
      }
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipelineApproverAccess

Beschreibung: Ermöglicht den Zugriff auf das Anzeigen und Genehmigen manueller Änderungen für alle Pipelines

`AWSCodePipelineApproverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodePipelineApproverAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Juli 2016, 18:59 Uhr UTC
- Bearbeitete Zeit: 2. August 2017, 17:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineApproverAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:PutApprovalResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodePipelineCustomActionAccess

Beschreibung: Ermöglicht den Zugriff auf benutzerdefinierte Aktionen zum Abrufen von Auftragsdetails (einschließlich temporärer Anmeldeinformationen) und zum Melden von Statusaktualisierungen AWS CodePipeline.

`AWSCodePipelineCustomActionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodePipelineCustomActionAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:02 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodePipelineCustomActionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Action" : [
        "codepipeline:AcknowledgeJob",
        "codepipeline:GetJobDetails",
        "codepipeline:PollForJobs",
        "codepipeline:PutJobFailureResult",
        "codepipeline:PutJobSuccessResult"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
```

```
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS CodeStar über die AWS-Managementkonsole.

`AWSCodeStarFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeStarFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. April 2017, 16:23 UTC
- Bearbeitete Zeit: 28. März 2023, 00:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCodeStarFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CodeStarEC2",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "cloud9:DescribeEnvironment*",
        "cloud9:ValidateEnvironmentName"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarCF",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStack*",
        "cloudformation:ListStacks*",
        "cloudformation:GetTemplateSummary"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarNotificationsServiceRolePolicy

Beschreibung: Ermöglicht AWS CodeStar Notifications den Zugriff auf Amazon CloudWatch Events in Ihrem Namen

`AWSCodeStarNotificationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. November 2019, 16:10 UTC
- Bearbeitete Zeit: 19. März 2020, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSCodeStarNotificationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/awscodestarnotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:CodeStarNotifications-*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommentsForComparedCommit",
        "chatbot:DescribeSlackChannelConfigurations",
        "chatbot:UpdateSlackChannelConfiguration",
        "codecommit:GetDifferences",
        "codepipeline:ListActionExecutions"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Action" : [
        "codecommit:GetFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/ExcludeFileContentFromNotifications" : "true"
        }
      },
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCodeStarServiceRole

Beschreibung: NICHT VERWENDEN — AWS CodeStar Service Role Policy, die Administratorrechte für CodeStar die Verwaltung von IAM und anderen Serviceressourcen im Namen des Kunden gewährt.

`AWSCodeStarServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCodeStarServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. April 2017, 15:20 Uhr UTC
- Bearbeitete Zeit: 20. September 2021, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCodeStarServiceRole`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ProjectEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:RemoveTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectStack",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*Stack*",
        "cloudformation:CreateChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awscodestar-*",
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/aws-cloud9-*",
        "arn:aws:cloudformation:*:aws:transform/CodeStar*"
      ]
    },
    {
      "Sid" : "ProjectStackTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectQuickstarts",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awscodestar-*/*"
      ]
    },
    {
      "Sid" : "ProjectS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-codestar-*",
        "arn:aws:s3:::elasticbeanstalk-*"
      ]
    },
    {
      "Sid" : "ProjectServices",
      "Effect" : "Allow",
      "Action" : [
        "codestar:*",
        "codecommit:*",
        "codepipeline:*",
        "codedeploy:*",
        "codebuild:*",
        "autoscaling:*",
        "cloudwatch:Put*",
        "ec2:*",
        "elasticbeanstalk:*",
        "elasticloadbalancing:*",
        "iam:ListRoles",
        "logs:*",
        "sns:*",
        "cloud9:CreateEnvironmentEC2",
        "cloud9:DeleteEnvironment",
        "cloud9:DescribeEnvironment*",
        "cloud9:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectWorkerRoles",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:PassRole",
        "iam:GetRolePolicy",
        "iam:PutRolePolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CodeStarWorker*",
        "arn:aws:iam::*:policy/CodeStarWorker*",
        "arn:aws:iam::*:instance-profile/awscodestar-*"
      ]
    },
    {
      "Sid" : "ProjectTeamMembers",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachUserPolicy",
        "iam:DetachUserPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyArn" : [
            "arn:aws:iam::*:policy/CodeStar_*"
          ]
        }
      }
    },
    {
      "Sid" : "ProjectRoles",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions",
        "iam:GetPolicy",
        "iam:GetPolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/CodeStar_*"
      ]
    },
    {
      "Sid" : "InspectServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-codestar-service-role",
        "arn:aws:iam::*:role/service-role/aws-codestar-service-role"
      ]
    },
    {
      "Sid" : "IAMLinkRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloud9.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeConfigRuleForARN",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ProjectCodeStarConnections",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codestar-connections:GetConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ProjectCodeStarConnectionsPassConnections",
      "Effect" : "Allow",
      "Action" : "codestar-connections:PassConnection",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "codestar-connections:PassedToService" : "codepipeline.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCompromisedKeyQuarantine

Beschreibung: Verweigert den Zugriff auf bestimmte Aktionen, die vom AWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich

zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Folgen Sie stattdessen den Anweisungen in der E-Mail, die Sie zu dieser Veranstaltung erhalten haben.

`AWSCompromisedKeyQuarantine`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCompromisedKeyQuarantine` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. August 2020, 18:04 UTC
- Bearbeitete Zeit: 11. August 2020, 18:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantine`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
```

```
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateUser",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "lambda:CreateFunction",
        "lightsail:Create*",
        "lightsail:Start*",
        "lightsail:Delete*",
        "lightsail:Update*",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:DownloadDefaultKeyPair"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCompromisedKeyQuarantineV2

Beschreibung: Verweigert den Zugriff auf bestimmte Aktionen, die vom AWS Team angewendet werden, falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Entfernen Sie diese Richtlinie NICHT. Folgen Sie stattdessen den Anweisungen in der für Sie erstellten Support-Anfrage zu dieser Veranstaltung.

`AWSCompromisedKeyQuarantineV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCompromisedKeyQuarantineV2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. April 2021, 22:30 Uhr UTC
- Bearbeitete Zeit: 2. Oktober 2024, 16:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV2`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
```

```
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
```

```
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCompromisedKeyQuarantineV3

Beschreibung: Verweigert den Zugriff auf bestimmte Aktionen, die angewendet werden AWS , falls die Anmeldeinformationen eines IAM-Benutzers kompromittiert oder öffentlich zugänglich gemacht wurden. Die Richtlinie zielt darauf ab, den potenziellen Schaden zu begrenzen, der durch betrügerische Aktivitäten verursacht werden kann, die zu nicht autorisierten Gebühren führen, ohne dass die vorhandenen Ressourcen beeinträchtigt werden. Entfernen Sie diese Richtlinie NICHT. Folgen Sie stattdessen den Anweisungen in der für Sie erstellten Support-Anfrage zu dieser Veranstaltung.

`AWSCompromisedKeyQuarantineV3`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCompromisedKeyQuarantineV3` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. August 2024, 17:36 UTC
- Bearbeitete Zeit: 2. Oktober 2024, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSCompromisedKeyQuarantineV3`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Deny",
      "Action" : [
        "cloudtrail:LookupEvents",
        "ec2:RequestSpotInstances",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:ChangePassword",
        "iam:CreateAccessKey",
        "iam:CreateInstanceProfile",
        "iam:CreateLoginProfile",
        "iam:CreatePolicyVersion",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:DetachUserPolicy",
        "iam:PassRole",
        "iam:PutGroupPolicy",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:SetDefaultPolicyVersion",
        "iam:UpdateAccessKey",
        "iam:UpdateAccountPasswordPolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateLoginProfile",
```

```
        "iam:UpdateUser",
        "lambda:AddLayerVersionPermission",
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetPolicy",
        "lambda:ListTags",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lightsail:Create*",
        "lightsail:Delete*",
        "lightsail:DownloadDefaultKeyPair",
        "lightsail:GetInstanceAccessDetails",
        "lightsail:Start*",
        "lightsail:Update*",
        "organizations:CreateAccount",
        "organizations:CreateOrganization",
        "organizations:InviteAccountToOrganization",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketAcl",
        "s3:PutBucketOwnershipControls",
        "s3:DeleteBucketPolicy",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:ListAllMyBuckets",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:AcceptReservedInstancesExchangeQuote",
        "ec2:CreateReservedInstancesListing",
        "savingsplans:CreateSavingsPlan",
        "ecs:CreateService",
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition",
        "ecr:GetAuthorizationToken",
        "bedrock:CreateModelInvocationJob",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:CreateFoundationModelAgreement",
        "bedrock:PutFoundationModelEntitlement",
        "bedrock:InvokeModel",
        "s3:CreateBucket",
```

```
        "s3:PutBucketCors",
        "s3:GetObject",
        "s3:ListBucket",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateProcessingJob",
        "ses:GetSendQuota",
        "ses:ListIdentities",
        "sts:GetSessionToken",
        "sts:GetFederationToken",
        "amplify:CreateDeployment",
        "amplify:CreateBackendEnvironment",
        "codebuild:CreateProject",
        "glue:CreateJob",
        "iam:DeleteRole",
        "iam:DeleteAccessKey",
        "iam:ListUsers",
        "lambda:GetEventSourceMapping",
        "sns:GetSMSAttributes",
        "mediapackagev2:CreateChannel"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigMultiAccountSetupPolicy

Beschreibung: Ermöglicht Config, AWS Dienste aufzurufen und Konfigurationsressourcen unternehmensweit bereitzustellen

`AWSConfigMultiAccountSetupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Juni 2019, 18:03 UTC
- Bearbeitete Zeit: 24. Februar 2023, 01:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigMultiAccountSetupPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
multiaccountsetup.amazonaws.com/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Resource" : "arn:aws:config:*:*:conformance-pack/aws-service-conformance-pack/
config-multiaccountsetup.amazonaws.com/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRemediationServiceRolePolicy

Beschreibung: Ermöglicht AWS Config, nicht konforme Ressourcen in Ihrem Namen zu korrigieren.

`AWSConfigRemediationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Juni 2019, 21:21 Uhr UTC
- Bearbeitete Zeit: 18. Juni 2019, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigRemediationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      },
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRoleForOrganizations

Beschreibung: Ermöglicht AWS Config, schreibgeschützte Organizations AWS aufzurufen APIs

`AWSConfigRoleForOrganizations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSConfigRoleForOrganizations` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. März 2018, 22:53 Uhr UTC
- Zeit bearbeitet: 24. November 2020, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigRulesExecutionRole

Beschreibung: Ermöglicht einer AWS Lambda-Funktion den Zugriff auf die AWS Config-API und die Konfigurations-Snapshots, die AWS Config regelmäßig an Amazon S3 übermittelt. Dieser Zugriff ist für Funktionen erforderlich, die Konfigurationsänderungen für benutzerdefinierte Konfigurationsregeln auswerten.

`AWSConfigRulesExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSConfigRulesExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. März 2016, 17:59 Uhr UTC
- Bearbeitete Zeit: 13. Mai 2019, 21:33 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSConfigRulesExecutionRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/AWSLogs/*/Config/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Put*",
        "config:Get*",
        "config:List*",
        "config:Describe*",
        "config:BatchGet*",
        "config:Select*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigServiceRolePolicy

Beschreibung: Ermöglicht Config, in Ihrem Namen AWS Dienste aufzurufen und Ressourcenkonfigurationen zu sammeln.

`AWSConfigServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. Mai 2018, 23:31 UTC
- Bearbeitete Zeit: 21. November 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSConfigServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v63 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSConfigServiceRolePolicyStatementID",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListTagsForResource",
        "account:GetAlternateContact",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListTags",
        "acm:DescribeCertificate",
        "acm:GetAccountConfiguration",
        "acm:ListCertificates",
        "acm:ListTagsForCertificate",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListTagsForResource",
        "amplifyuibuilder:ExportThemes",
        "amplifyuibuilder:GetTheme",
        "amplifyuibuilder:ListForms",
        "amplifyuibuilder:ListThemes",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
```

```
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListVpcEndpoints",
        "app-integrations:GetApplication",
        "app-integrations:GetDataIntegration",
        "app-integrations:GetEventIntegration",
        "app-integrations:ListApplications",
        "app-integrations:ListDataIntegrations",
        "app-integrations:ListEventIntegrationAssociations",
        "app-integrations:ListEventIntegrations",
        "app-integrations:ListTagsForResource",
        "appconfig:GetApplication",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetExtensionAssociation",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeployments",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeFlow",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListServiceLevelObjectives",
```

```
        "application-signals:ListTagsForResource",
        "appmesh:DescribeGatewayRoute",
        "appmesh:DescribeMesh",
        "appmesh:DescribeRoute",
        "appmesh:DescribeVirtualGateway",
        "appmesh:DescribeVirtualNode",
        "appmesh:DescribeVirtualRouter",
        "appmesh:DescribeVirtualService",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListTagsForResource",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlockBuilders",
        "appstream:DescribeApplications",
        "appstream:DescribeDirectoryConfigs",
        "appstream:DescribeFleets",
        "appstream:DescribeStacks",
        "appstream:ListTagsForResource",
        "appsync:GetApiCache",
        "appsync:GetGraphqlApi",
        "appsync:GetSourceApiAssociation",
        "appsync:ListGraphqlApis",
        "appsync:ListSourceApiAssociations",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "APS:DescribeRuleGroupsNamespace",
        "APS:DescribeWorkspace",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListTagsForResource",
        "APS:ListWorkspaces",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:ListAutoScalingConfigurations",
```

```
        "apprunner:ListVpcIngressConnections",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeImageBuilders",
        "appsync:GetApi",
        "appsync:GetDomainName",
        "appsync:ListApis",
        "appsync:ListDomainNames",
        "appsync:ListTagsForResource",
        "apptest:GetTestCase",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "aps:DescribeScraper",
        "aps:DescribeScraperLoggingConfiguration",
        "aps:ListScrapers",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "athena:GetDataCatalog",
        "athena:GetPreparedStatement",
        "athena:GetWorkGroup",
        "athena:ListDataCatalogs",
        "athena:ListPreparedStatements",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:ListAssessments",
        "autoscaling-plans:DescribeScalingPlanResources",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DescribeTags",
        "autoscaling:DescribeWarmPool",
        "b2bi:GetCapability",
        "b2bi:GetPartnership",
        "b2bi:GetProfile",
        "b2bi:GetTransformer",
        "b2bi:ListCapabilities",
        "b2bi:ListPartnerships",
        "b2bi:ListProfiles",
        "b2bi:ListTagsForResource",
        "b2bi:ListTransformers",
```

```
        "backup-gateway:GetHypervisor",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:DescribeBackupVault",
        "backup:DescribeFramework",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeReportPlan",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:GetRestoreTestingPlan",
        "backup:GetRestoreTestingSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListFrameworks",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListReportPlans",
        "backup:ListRestoreTestingPlans",
        "backup:ListRestoreTestingSelections",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobQueues",
        "batch:DescribeSchedulingPolicies",
        "batch:ListSchedulingPolicies",
        "batch:ListTagsForResource",
        "bcm-data-exports:GetExport",
        "bcm-data-exports:ListExports",
        "bcm-data-exports:ListTagsForResource",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListTagsForResource",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
```

```
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataSource",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListDataSources",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListTagsForResource",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:ViewBudget",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListTrainingDatasets",
```

```
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListTagsForResource",
        "cloud9:DescribeEnvironmentMemberships",
        "cloud9:DescribeEnvironments",
        "cloud9:ListEnvironments",
        "cloud9:ListTagsForResource",
        "cloudformation:BatchDescribeTypeConfigurations",
        "cloudformation:DescribePublisher",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeType",
        "cloudformation:GetResource",
        "cloudformation:ListResources",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
        "cloudformation:ListTypes",
        "cloudfront:DescribeFunction",
        "cloudfront:DescribeKeyValueStore",
        "cloudfront:GetConnectionGroup",
        "cloudfront:GetFunction",
        "cloudfront:GetOriginAccessControl",
        "cloudfront:GetPublicKey",
        "cloudfront:GetRealtimeLogConfig",
        "cloudfront:GetResponseHeadersPolicy",
        "cloudfront:ListDistributions",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListPublicKeys",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudfront:ListTagsForResource",
        "cloudtrail:DescribeTrails",
        "cloudTrail:GetChannel",
        "cloudtrail:GetEventConfiguration",
```

```
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetResourcePolicy",
        "cloudtrail:GetTrailStatus",
        "cloudTrail:ListChannels",
        "cloudfront:GetDistributionTenant",
        "cloudfront:GetVpcOrigin",
        "cloudfront:ListConnectionGroups",
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListKeyValueStores",
        "cloudfront:ListVpcOrigins",
        "cloudtrail:GetDashboard",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAnomalyDetectors",
        "cloudwatch:GetDashboard",
        "cloudwatch:GetMetricStream",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "cloudwatch:ListTagsForResource",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackageGroup",
        "codeartifact:DescribeRepository",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListAllowedRepositoriesForGroup",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageGroups",
        "codeartifact:ListPackages",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListRepositories",
        "codeartifact:ListTagsForResource",
        "codebuild:BatchGetReportGroups",
        "codebuild:ListReportGroups",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:ListRepositories",
        "codecommit:ListTagsForResource",
        "codeconnections:GetConnection",
```

```
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codedeploy:GetDeploymentConfig",
        "codeguru-profiler:DescribeProfilingGroup",
        "codeguru-profiler:GetNotificationConfiguration",
        "codeguru-profiler:GetPolicy",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:DescribeRepositoryAssociation",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:ListTagsForResource",
        "codepipeline:ListWebhooks",
        "codestar-connections:GetConnection",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:ListConnections",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListTagsForResource",
        "cognito-identity:DescribeIdentityPool",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetPrincipalTagAttributeMap",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:DescribeIdentityProvider",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolClient",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:GetGroup",
        "cognito-idp:GetUserPoolMfaConfig",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "comprehend:DescribeFlywheel",
        "comprehend:ListFlywheels",
        "comprehend:ListTagsForResource",
        "config:BatchGet*",
        "config:Describe*",
        "config:Get*",
```

```
        "config:List*",
        "config:Put*",
        "config:Select*",
        "connect:DescribeEvaluationForm",
        "connect:DescribeInstance",
        "connect:DescribeInstanceStorageConfig",
        "connect:DescribePhoneNumber",
        "connect:DescribePredefinedAttribute",
        "connect:DescribePrompt",
        "connect:DescribeQueue",
        "connect:DescribeQuickConnect",
        "connect:DescribeRoutingProfile",
        "connect:DescribeRule",
        "connect:DescribeSecurityProfile",
        "connect:DescribeTrafficDistributionGroup",
        "connect:DescribeUser",
        "connect:DescribeView",
        "connect:GetTaskTemplate",
        "connect:ListApprovedOrigins",
        "connect:ListEvaluationForms",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListPhoneNumbers",
        "connect:ListPhoneNumbersV2",
        "connect:ListPredefinedAttributes",
        "connect:ListPrompts",
        "connect:ListQueueQuickConnects",
        "connect:ListQueues",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityKeys",
        "connect:ListSecurityProfileApplications",
        "connect:ListSecurityProfilePermissions",
        "connect:ListSecurityProfiles",
        "connect:ListTagsForResource",
        "connect:ListTaskTemplates",
        "connect:ListTrafficDistributionGroups",
        "connect:ListUsers",
        "connect:ListViewVersions",
        "connect:ListViews",
```

```
        "connect:SearchAvailablePhoneNumbers",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "datasync:DescribeAgent",
        "datasync:DescribeLocationEfs",
        "datasync:DescribeLocationFsxLustre",
        "datasync:DescribeLocationFsxWindows",
        "datasync:DescribeLocationHdfs",
        "datasync:DescribeLocationNfs",
        "datasync:DescribeLocationObjectStorage",
        "datasync:DescribeLocationS3",
        "datasync:DescribeLocationSmb",
        "datasync:DescribeTask",
        "datasync:ListAgents",
        "datasync:ListLocations",
        "datasync:ListTagsForResource",
        "datasync:ListTasks",
        "datazone:GetDomain",
        "datazone:ListDomains",
        "dax:DescribeClusters",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetMonitor",
        "deadline:GetQueueFleetAssociation",
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListMonitors",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListTagsForResource",
```

```
        "detective:ListGraphs",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "devicefarm:GetInstanceProfile",
        "devicefarm:GetNetworkProfile",
        "devicefarm:GetProject",
        "devicefarm:GetTestGridProject",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListNetworkProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTagsForResource",
        "devicefarm:ListTestGridProjects",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListNotificationChannels",
        "directconnect:DescribeConnections",
        "dms:DescribeCertificates",
        "dms:DescribeDataMigrations",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationConfigs",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTaskAssessmentRuns",
        "dms:DescribeReplicationTasks",
        "dms:ListMigrationProjects",
        "dms:ListTagsForResource",
        "ds:DescribeDirectories",
        "ds:DescribeDomainControllers",
        "ds:DescribeEventTopics",
        "ds:ListLogSubscriptions",
        "ds:ListTagsForResource",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetInstanceTypesFromInstanceRequirements",
```

```
        "ec2:GetIpamPoolAllocations",
        "ec2:GetIpamPoolCidrs",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetVerifiedAccessGroupPolicy",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayMulticastGroups",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribePullThroughCacheRules",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:DescribeRepositoryCreationTemplates",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListTagsForResource",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListServices",
        "ecs:ListTagsForResource",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:DescribePodIdentityAssociation",
        "eks:ListAccessEntries",
        "eks:ListAddons",
        "eks:ListAssociatedAccessPolicies",
        "eks:ListClusters",
```

```
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "eks:ListTagsForResource",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheParameters",
        "elasticache:DescribeCacheSecurityGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeConfigurationSettings",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribeSecurityConfiguration",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:DescribeStudio",
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetStudioSessionMapping",
```

```
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elasticmapreduce:ListSteps",
        "elasticmapreduce:ListStudios",
        "elasticmapreduce:ListStudioSessionMappings",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdMappingWorkflow",
        "entityresolution:GetMatchingWorkflow",
        "entityresolution:GetSchemaMapping",
        "entityresolution:ListIdMappingWorkflows",
        "entityresolution:ListMatchingWorkflows",
        "entityresolution:ListSchemaMappings",
        "entityresolution:ListTagsForResource",
        "es:DescribeDomain",
        "es:DescribeDomains",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:GetCompatibleElasticsearchVersions",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListTags",
        "events:DescribeApiDestination",
        "events:DescribeArchive",
        "events:DescribeConnection",
        "events:DescribeEndpoint",
        "events:DescribeEventBus",
        "events:DescribeRule",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
```

```
        "events:ListRules",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "finspace:GetEnvironment",
        "finspace:ListEnvironments",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "firehose:ListTagsForDeliveryStream",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:ListPolicies",
        "fms:ListTagsForResource",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasets",
        "forecast:ListTagsForResource",
        "frauddetector:GetDetectors",
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeDataRepositoryAssociations",
        "fsx:DescribeFileSystems",
        "fsx:DescribeSnapshots",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
```

```
        "gamelift:DescribeAlias",
        "gamelift:DescribeBuild",
        "gamelift:DescribeContainerGroupDefinition",
        "gamelift:DescribeFleetAttributes",
        "gamelift:DescribeFleetCapacity",
        "gamelift:DescribeFleetLocationAttributes",
        "gamelift:DescribeFleetLocationCapacity",
        "gamelift:DescribeFleetPortSettings",
        "gamelift:DescribeGameServerGroup",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:DescribeRuntimeConfiguration",
        "gamelift:DescribeScript",
        "gamelift:DescribeVpcPeeringAuthorizations",
        "gamelift:DescribeVpcPeeringConnections",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListContainerGroupDefinitions",
        "gamelift:ListFleets",
        "gamelift:ListGameServerGroups",
        "gamelift:ListScripts",
        "gamelift:ListTagsForResource",
        "geo:DescribeGeofenceCollection",
        "geo:DescribeKey",
        "geo:DescribeMap",
        "geo:DescribePlaceIndex",
        "geo:DescribeRouteCalculator",
        "geo:DescribeTracker",
        "geo:ListGeofenceCollections",
        "geo:ListKeys",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListRouteCalculators",
        "geo:ListTrackerConsumers",
        "geo:ListTrackers",
        "globalaccelerator:DescribeAccelerator",
        "globalaccelerator:DescribeCrossAccountAttachment",
        "globalaccelerator:DescribeEndpointGroup",
        "globalaccelerator:DescribeListener",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListCrossAccountAttachments",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
```

```
        "globalaccelerator:ListTagsForResource",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetRegistry",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTable",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetWorkflow",
        "glue:ListCrawlers",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:GetComponent",
        "greengrass:ListComponents",
        "greengrass:ListComponentVersions",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMissionProfile",
```

```
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "groundstation:ListTagsForResource",
        "guardduty:DescribePublishingDestination",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
        "guardduty:GetIPSet",
        "guardduty:GetMalwareProtectionPlan",
        "guardduty:GetMasterAccount",
        "guardduty:GetMemberDetectors",
        "guardduty:GetMembers",
        "guardduty:GetThreatIntelSet",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListFindings",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListMembers",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListTagsForResource",
        "guardduty:ListThreatIntelSets",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListTagsForResource",
        "iam:GenerateCredentialReport",
        "iam:GetAccountAuthorizationDetails",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetGroup",
        "iam:GetGroupPolicy",
        "iam:GetInstanceProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:GetSAMLProvider",
        "iam:GetServerCertificate",
        "iam:GetUser",
```

```
        "iam:GetUserPolicy",
        "iam:ListAccessKeys",
        "iam:ListAttachedGroupPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListAttachedUserPolicies",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroups",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles",
        "iam:ListInstanceProfilesForRole",
        "iam:ListInstanceProfileTags",
        "iam:ListMFADevices",
        "iam:ListMFADeviceTags",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUserPolicies",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "imagebuilder:GetDistributionConfiguration",
        "imagebuilder:GetImage",
        "imagebuilder:GetImagePipeline",
        "imagebuilder:GetImageRecipe",
        "imagebuilder:GetInfrastructureConfiguration",
        "imagebuilder:GetLifecyclePolicy",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
```

```
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "imagebuilder:ListLifecyclePolicies",
        "inspector2:BatchGetAccountStatus",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:ListFilters",
        "inspector2:ListMembers",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuthorizer",
        "iot:DescribeBillingGroup",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeCertificateProvider",
        "iot:DescribeCustomMetric",
        "iot:DescribeDimension",
        "iot:DescribeDomainConfiguration",
        "iot:DescribeFleetMetric",
        "iot:DescribeJobTemplate",
        "iot:DescribeMitigationAction",
        "iot:DescribeProvisioningTemplate",
        "iot:DescribeRoleAlias",
        "iot:DescribeScheduledAudit",
        "iot:DescribeSecurityProfile",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:GetPackage",
        "iot:GetPackageVersion",
        "iot:GetPolicy",
        "iot:GetTopicRule",
        "iot:GetTopicRuleDestination",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificateProviders",
        "iot:ListCertificates",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListDomainConfigurations",
        "iot:ListFleetMetrics",
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
```

```
        "iot:ListPackageVersions",
        "iot:ListPackages",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTagsForResource",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:ValidateSecurityProfileBehaviors",
        "iotanalytics:DescribeChannel",
        "iotanalytics:DescribeDataset",
        "iotanalytics:DescribeDatastore",
        "iotanalytics:DescribePipeline",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotanalytics:ListTagsForResource",
        "iotdeviceadvisor:GetSuiteDefinition",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListModelManifestNodes",
```

```
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
        "iotfleetwise:ListVehicles",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:GetEntity",
        "iottwinmaker:GetScene",
        "iottwinmaker:GetSyncJob",
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListScenes",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListTagsForResource",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessGateway",
```

```
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGateways",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "ivs:GetChannel",
        "ivs:GetEncoderConfiguration",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStorageConfiguration",
        "ivs:GetStreamKey",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:DescribeVpcConnection",
        "kafka:GetClusterPolicy",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurations",
        "kafka:ListScramSecrets",
```

```
        "kafka:ListTagsForResource",
        "kafka:ListVpcConnections",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListTagsForResource",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:DescribeIndex",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetResourcePolicy",
        "kinesis:ListStreamConsumers",
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:DescribeKey",
        "kms:GetKeyPolicy",
        "kms:GetKeyRotationStatus",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lakeformation:DescribeLakeFormationIdentityCenterConfiguration",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lambda:GetAlias",
        "lambda:GetCodeSigningConfig",
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:GetFunctionCodeSigningConfig",
```

```
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionUrlConfig",
        "lambda:GetLayerVersion",
        "lambda:GetPolicy",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetRuntimeManagementConfig",
        "lambda:ListAliases",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListFunctionUrlConfigs",
        "lambda:ListFunctions",
        "lambda:ListLayers",
        "lambda:ListLayerVersions",
        "lambda:ListTags",
        "lambda:ListVersionsByFunction",
        "launchwizard:GetDeployment",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListTagsForResource",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotVersion",
        "lex:DescribeResourcePolicy",
        "lex:ListBotAliases",
        "lex:ListBotLocales",
        "lex:ListBots",
        "lex:ListBotVersions",
        "lex:ListTagsForResource",
        "license-manager:GetGrant",
        "license-manager:GetLicense",
        "license-manager:ListDistributedGrants",
        "license-manager:ListLicenses",
        "license-manager:ListReceivedGrants",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDisks",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
```

```
        "lightsail:GetInstance",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancers",
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetOperations",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "logs:DescribeAccountPolicies",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliveryDestinations",
        "logs:DescribeDeliverySources",
        "logs:DescribeDestinations",
        "logs:DescribeIndexPolicies",
        "logs:DescribeLogGroups",
        "logs:DescribeMetricFilters",
        "logs:DescribeResourcePolicies",
        "logs:GetDataProtectionPolicy",
        "logs:GetDelivery",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:GetDeliverySource",
        "logs:GetLogAnomalyDetector",
        "logs:GetLogDelivery",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:DescribeAlert",
        "lookoutmetrics:DescribeAnomalyDetector",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutmetrics:ListMetricSets",
        "lookoutmetrics:ListTagsForResource",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListProjects",
```

```
        "m2:GetEnvironment",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetMacieSession",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListTagsForResource",
        "managedblockchain:GetAccessor",
        "managedblockchain:GetMember",
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:ListAccessors",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNodes",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeGateway",
        "mediaconnect:ListBridges",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGateways",
        "mediaconnect:ListTagsForResource",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeMultiplexProgram",
        "medialive:ListChannelPlacementGroups",
        "medialive:ListMultiplexPrograms",
        "medialive:ListMultiplexes",
        "medialive:ListTagsForResource",
        "mediapackage-vod:DescribeAsset",
        "mediapackage-vod:DescribePackagingConfiguration",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage-vod:ListTagsForResource",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
```

```
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediatailor:DescribeChannel",
        "mediatailor:DescribeLiveSource",
        "mediatailor:DescribeSourceLocation",
        "mediatailor:DescribeVodSource",
        "mediatailor:GetPlaybackConfiguration",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeParameters",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListTags",
        "mobiletargeting:GetApp",
        "mobiletargeting:GetApplicationSettings",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaign",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetEmailChannel",
        "mobiletargeting:GetEmailTemplate",
        "mobiletargeting:GetEventStream",
        "mobiletargeting:GetInAppTemplate",
        "mobiletargeting:GetSegment",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTagsForResource",
        "mobiletargeting:ListTemplates",
        "mq:DescribeBroker",
        "mq:ListBrokers",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:ListFirewalls",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
```

```
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetStreamingImage",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStudioComponents",
        "nimble:ListStudios",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListSinks",
        "omics:GetAnnotationStore",
        "omics:GetRunGroup",
        "omics:GetSequenceStore",
        "omics:GetVariantStore",
        "omics:GetWorkflow",
        "omics:ListAnnotationStores",
        "omics:ListRunGroups",
        "omics:ListSequenceStores",
        "omics:ListTagsForResource",
        "omics:ListVariantStores",
        "omics:ListWorkflows",
        "opsworks:DescribeInstances",
        "opsworks:DescribeLayers",
        "opsworks:DescribeTimeBasedAutoScaling",
        "opsworks:DescribeVolumes",
        "opsworks:ListTags",
        "organizations:DescribeAccount",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListTagsForResource",
        "organizations:ListTargetsForPolicy",
        "osis:GetPipeline",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "panorama:DescribeApplicationInstance",
        "panorama:DescribeApplicationInstanceDetails",
        "panorama:DescribePackage",
        "panorama:DescribePackageVersion",
        "panorama:ListApplicationInstances",
        "panorama:ListNodes",
        "panorama:ListPackages",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "personalize:DescribeDataset",
        "personalize:DescribeDatasetGroup",
        "personalize:DescribeSchema",
        "personalize:DescribeSolution",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasetImportJobs",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "personalize:ListTagsForResource",
        "pipes:DescribePipe",
        "pipes:ListPipes",
        "profile:GetDomain",
        "profile:GetIntegration",
```

```
        "profile:GetProfileObjectType",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "profile:ListTagsForResource",
        "qbusiness:GetApplication",
        "qbusiness:ListApplications",
        "qbusiness:ListTagsForResource",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DescribeTemplate",
        "quicksight:DescribeTemplatePermissions",
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions",
        "quicksight:DescribeTopic",
        "quicksight:ListAnalyses",
        "quicksight:ListDashboards",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListRefreshSchedules",
        "quicksight:ListTagsForResource",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "quicksight:ListTopics",
        "ram:GetPermission",
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares",
        "ram:ListPermissionAssociations",
        "ram:ListPermissions",
        "ram:ListPermissionVersions",
        "ram:ListResources",
        "ram:ListResourceSharePermissions",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusters",
```

```
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBProxyTargetGroups",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBShardGroups",
        "rds:DescribeDBSnapshotAttributes",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeIntegrations",
        "rds:DescribeOptionGroups",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeEndpointAccess",
        "redshift:DescribeEndpointAuthorization",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeIntegrations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeTags",
        "redshift:GetResourcePolicy",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetService",
```

```
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:ListStreamProcessors",
        "rekognition:ListTagsForResource",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:ListApps",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetTags",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "robomaker:DescribeRobotApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListRobotApplications",
        "robomaker:ListSimulationApplications",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-control-config:DescribeCluster",
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeRoutingControl",
        "route53-recovery-control-config:DescribeSafetyRule",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-control-config:ListTagsForResource",
```

```
        "route53-recovery-readiness:GetCell",
        "route53-recovery-readiness:GetReadinessCheck",
        "route53-recovery-readiness:GetRecoveryGroup",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:GetChange",
        "route53:GetDNSSEC",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListCidrBlocks",
        "route53:ListCidrCollections",
        "route53:ListCidrLocations",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListQueryLoggingConfigs",
        "route53:ListResourceRecordSets",
        "route53:ListTagsForResource",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:GetFirewallDomainList",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetResolverDnssecConfig",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:GetResolverQueryLogConfigAssociation",
        "route53resolver:GetResolverRule",
        "route53resolver:GetResolverRuleAssociation",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallDomains",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListFirewallRules",
        "route53resolver:ListResolverDnssecConfigs",
        "route53resolver:ListResolverEndpointIpAddresses",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigAssociations",
```

```
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRuleAssociations",
        "route53resolver:ListResolverRules",
        "route53resolver:ListTagsForResource",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:ListTagsForResource",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListRegionalBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrant",
        "s3:GetAccessGrantsInstance",
        "s3:GetAccessGrantsLocation",
        "s3:GetAccessPoint",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketAbac",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketNotification",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
```

```
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetReplicationConfiguration",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensConfigurationTagging",
        "s3:GetStorageLensGroup",
        "s3:ListAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrantsLocations",
        "s3:ListAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3:ListTagsForResource",
        "s3express:GetBucketPolicy",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetLifecycleConfiguration",
        "s3express:ListAllMyDirectoryBuckets",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:ListTableBuckets",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeAppImageConfig",
        "sagemaker:DescribeCluster",
        "sagemaker:DescribeCodeRepository",
        "sagemaker:DescribeDataQualityJobDefinition",
        "sagemaker:DescribeDeviceFleet",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeFeatureGroup",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceExperiment",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelBiasJobDefinition",
```

```
        "sagemaker:DescribeModelCard",
        "sagemaker:DescribeModelExplainabilityJobDefinition",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeModelQualityJobDefinition",
        "sagemaker:DescribeMonitoringSchedule",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeProject",
        "sagemaker:DescribeStudioLifecycleConfig",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeWorkteam",
        "sagemaker:GetModelPackageGroupPolicy",
        "sagemaker:ListAppImageConfigs",
        "sagemaker:ListApps",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListDataQualityJobDefinitions",
        "sagemaker:ListDeviceFleets",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListImages",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelBiasJobDefinitions",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelExplainabilityJobDefinitions",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelQualityJobDefinitions",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListProjects",
```

```
            "sagemaker:ListStudioLifecycleConfigs",
            "sagemaker:ListTags",
            "sagemaker:ListUserProfiles",
            "sagemaker:ListWorkteams",
            "scheduler:GetSchedule",
            "scheduler:GetScheduleGroup",
            "scheduler:ListScheduleGroups",
            "scheduler:ListSchedules",
            "scheduler:ListTagsForResource",
            "schemas:DescribeDiscoverer",
            "schemas:DescribeRegistry",
            "schemas:DescribeSchema",
            "schemas:GetResourcePolicy",
            "schemas:ListDiscoverers",
            "schemas:ListRegistries",
            "schemas:ListSchemas",
            "sdb:GetAttributes",
            "sdb:ListDomains",
            "secretsmanager:DescribeSecret",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:ListSecrets",
            "secretsmanager:ListSecretVersionIds",
            "securityhub:DescribeHub",
            "securityhub:DescribeStandardsControls",
            "securityhub:GetEnabledStandards",
            "securitylake:GetSubscriber",
            "securitylake:ListDataLakeExceptions",
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers",
            "securitylake:ListTagsForResource",
            "serviceCatalog:DescribePortfolioShares",
            "servicecatalog:DescribeServiceAction",
            "servicecatalog:GetAttributeGroup",
            "servicecatalog:ListApplications",
            "servicecatalog:ListAssociatedResources",
            "servicecatalog:ListAttributeGroups",
            "servicecatalog:ListServiceActions",
            "servicecatalog:ListServiceActionsForProvisioningArtifact",
            "servicediscovery:GetInstance",
            "servicediscovery:GetNamespace",
            "servicediscovery:GetService",
            "servicediscovery:ListInstances",
            "servicediscovery:ListNamespaces",
```

```
        "servicediscovery:ListServices",
        "servicediscovery:ListTagsForResource",
        "ses:DescribeReceiptRule",
        "ses:DescribeReceiptRuleSet",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetContactList",
        "ses:GetDedicatedIpPool",
        "ses:GetDedicatedIps",
        "ses:GetEmailTemplate",
        "ses:GetTemplate",
        "ses:GetTrafficPolicy",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
        "ses:ListDedicatedIpPools",
        "ses:ListEmailTemplates",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListTagsForResource",
        "ses:ListTemplates",
        "ses:ListTrafficPolicies",
        "shield:DescribeDRTAccess",
        "shield:DescribeProtection",
        "shield:DescribeProtectionGroup",
        "shield:DescribeSubscription",
        "shield:ListProtectionGroups",
        "shield:ListTagsForResource",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningProfiles",
        "sns:GetDataProtectionPolicy",
        "sns:GetSMSSandboxAccountStatus",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm-contacts:GetContact",
        "ssm-contacts:GetContactChannel",
        "ssm-contacts:ListContactChannels",
```

```
            "ssm-contacts:ListContacts",
            "ssm-contacts:ListTagsForResource",
            "ssm-incidents:GetReplicationSet",
            "ssm-incidents:GetResponsePlan",
            "ssm-incidents:ListReplicationSets",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:ListTagsForResource",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-sap:ListTagsForResource",
            "ssm:DescribeAssociation",
            "ssm:DescribeAutomationExecutions",
            "ssm:DescribeDocument",
            "ssm:DescribeDocumentPermission",
            "ssm:DescribeInstanceInformation",
            "ssm:DescribeMaintenanceWindows",
            "ssm:DescribeParameters",
            "ssm:DescribePatchBaselines",
            "ssm:GetAutomationExecution",
            "ssm:GetDefaultPatchBaseline",
            "ssm:GetDocument",
            "ssm:GetPatchBaseline",
            "ssm:GetResourcePolicies",
            "ssm:GetServiceSetting",
            "ssm:ListAssociations",
            "ssm:ListDocuments",
            "ssm:ListResourceDataSync",
            "ssm:ListTagsForResource",
            "sso:DescribeInstanceAccessControlAttributeConfiguration",
            "sso:DescribePermissionSet",
            "sso:GetInlinePolicyForPermissionSet",
            "sso:ListManagedPoliciesInPermissionSet",
            "sso:ListPermissionSets",
            "sso:ListTagsForResource",
            "states:DescribeActivity",
            "states:DescribeStateMachine",
            "states:DescribeStateMachineAlias",
            "states:ListActivities",
            "states:ListStateMachineAliases",
            "states:ListStateMachines",
            "states:ListTagsForResource",
            "storagegateway:ListGateways",
            "storagegateway:ListTagsForResource",
            "storagegateway:ListVolumes",
```

```
        "sts:GetCallerIdentity",
        "support:DescribeCases",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListDatabases",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "transfer:DescribeAgreement",
        "transfer:DescribeCertificate",
        "transfer:DescribeConnector",
        "transfer:DescribeProfile",
        "transfer:DescribeServer",
        "transfer:DescribeUser",
        "transfer:DescribeWorkflow",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListTagsForResource",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "verifiedpermissions:ListTagsForResource",
        "voiceid:DescribeDomain",
        "voiceid:ListTagsForResource",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetService",
```

```
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:GetLoggingConfiguration",
        "waf-regional:GetWebACL",
        "waf-regional:GetWebACLForResource",
        "waf-regional:ListLoggingConfigurations",
        "waf:GetLoggingConfiguration",
        "waf:GetWebACL",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetRuleGroup",
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeTags",
        "workspaces:DescribeWorkspaces",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:ListResourcePolicies",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSConfigSLRLogStatementID",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*"
    },
    {
      "Sid" : "AWSConfigSLRLogEventStatementID",
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-
evaluation/*"
    },
    {
      "Sid" : "AWSConfigSLRApiGatewayStatementID",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes",
        "arn:aws:apigateway:*::/v2/apis/*/routes/*",
        "arn:aws:apigateway:*::/v2/apis",
        "arn:aws:apigateway:*::/v2/apis/*",
        "arn:aws:apigateway:*::/v2/apis/*/integrations",
        "arn:aws:apigateway:*::/v2/apis/*/integrations/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConfigUserAccess

Beschreibung: Ermöglicht den Zugriff auf die Verwendung von AWS Config, einschließlich der Suche nach Tags in Ressourcen und dem Lesen aller Tags. Dies gewährt keine Berechtigung zur Konfiguration von AWS Config, wofür Administratorrechte erforderlich sind.

`AWSConfigUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSConfigUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Februar 2015, 19:38 UTC
- Bearbeitete Zeit: 18. März 2019, 20:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConfigUserAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSConnector

Beschreibung: Ermöglicht read/write den umfassenden Zugriff auf ALLE EC2 Objekte, den read/write Zugriff auf S3-Buckets, die mit 'import-to-ec2' beginnen, und die Möglichkeit, alle S3-Buckets aufzulisten, damit der AWS Connector in Ihrem Namen importieren VMs kann.

`AWSConnector`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSConnector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2015, 17:14 Uhr UTC
- Zeit bearbeitet: 28. September 2015, 19:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSConnector`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
```

```
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : "arn:aws:s3:::import-to-ec2-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelConversionTask",
        "ec2:CancelExportTask",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteTags",
        "ec2:DeleteVolume",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeExportTasks",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:DetachVolume",
        "ec2:ImportInstance",
        "ec2:ImportVolume",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CancelImportTask",
        "ec2:ImportSnapshot",
```

```
        "ec2:DescribeImportSnapshotTasks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerAccountServiceRolePolicy

Beschreibung: Ermöglicht AWS Control Tower, AWS Dienste aufzurufen, die eine automatisierte Kontokonfiguration und zentrale Verwaltung in Ihrem Namen bereitstellen.

`AWSControlTowerAccountServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Juni 2023, 22:04 UTC

- Bearbeitete Zeit: 5. November 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSControlTowerAccountServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPutRuleOnSpecificSourcesAndDetailTypes",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "events:source" : "aws.securityhub"
        },
        "Null" : {
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com",
          "events:detail-type" : "Security Hub Findings - Imported"
        }
      }
    },
    {
      "Sid" : "AllowOtherOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
```

```
        "events:EnableRule",
        "events:DisableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "controltower.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDescribeOperationsOnRulesManagedByControlTower",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/*ControlTower*"
    },
    {
      "Sid" : "AllowControlTowerToPublishSecurityNotifications",
      "Effect" : "Allow",
      "Action" : "sns:publish",
      "Resource" : "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "AllowActionsForSecurityHubIntegration",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DescribeStandardsControls",
        "securityhub:GetEnabledStandards"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Sid" : "AllowDeleteConfigRule",
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowPutConfigRule",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*"
    },
    {
      "Sid" : "AllowConfigTagResource",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Sid" : "AllowConfigRulesDescribe",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowControlTowerToCreateConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToManageConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:DescribeAggregateComplianceByConfigRules",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/config-aggregator-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToTagConfigAggregator",
      "Effect" : "Allow",
      "Action" : [
        "config:TagResource"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
controltower.amazonaws.com/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/aws-control-tower" : "managed-by-control-tower",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowControlTowerToPassAggregatorRoleToConfig",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "config.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeConfigurationAggregators",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationAggregators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListDelegatedAdministratorsForConfig",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowListDescribeOrganization",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerCloudTrailRolePolicy

Beschreibung: AWS Control Tower dient AWS CloudTrail als bewährte Methode und bietet diese Rolle für AWS CloudTrail. AWS CloudTrail übernimmt diese Rolle für die Erstellung und Veröffentlichung von CloudTrail Protokollen

`AWSControlTowerCloudTrailRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSControlTowerCloudTrailRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 5. November 2025, 21:19 UTC
- Zeit bearbeitet: 5. November 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerCloudTrailRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogStream",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerIdentityCenterManagementPolicy

Beschreibung: Stellt Berechtigungen zur Verwaltung der IAM Identity Center (IdC) -Ressourcen in den bei Control Tower registrierten Mitgliedskonten bereit. AWS Die Richtlinie ist der AWSControl TowerAdmin Rolle nur dann zugeordnet, wenn der Kunde sich für die IAM-iDC-Integration in seiner AWS Control Tower Landing Zone entschieden hat.

`AWSControlTowerIdentityCenterManagementPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSControlTowerIdentityCenterManagementPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 03. Oktober 2025, 18:34 UTC
- Bearbeitete Zeit: 03. Oktober 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerIdentityCenterManagementPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AllowIdentityCenterInstancePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListPermissionSets"
      ],
      "Resource" : "arn:aws:sso:::instance/*"
    },
    {
      "Sid" : "AllowIdentityCenterManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:GetProfile",
        "sso:CreateProfile",
        "sso:UpdateProfile",
        "sso:GetTrust",
        "sso:CreateTrust",
        "sso:UpdateTrust",
        "sso:CreateApplicationInstance",
        "sso:GetApplicationInstance",
        "sso:GetSSOStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowIdentityCenterDirectoryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:SearchGroups",
        "sso-directory:CreateGroup",
        "sso-directory:SearchUsers",
        "sso-directory:CreateUser",
        "sso-directory:DescribeDirectory"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSControlTowerServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von AWS Control Tower verwaltet oder verwendet werden

`AWSControlTowerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSControlTowerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 03. Mai 2019, 18:19 Uhr UTC
- Bearbeitete Zeit: 5. November 2025, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackInstances",
        "cloudformation:UpdateStack",
```

```
        "cloudformation:UpdateStackInstances",
        "cloudformation:UpdateStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
        "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
        "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateTrail",
        "cloudtrail:DeleteTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail",
        "cloudtrail:PutEventSelectors",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs*:*",
        "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-controltower*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/AWSControlTowerExecution",
        "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "ec2:DescribeAvailabilityZones",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "organizations:CreateAccount",
        "organizations:DescribeAccount",
        "organizations:DescribeCreateAccountStatus",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListRoots",
        "organizations:MoveAccount",
        "servicecatalog:AssociatePrincipalWithPortfolio"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListAttachedRolePolicies",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
        "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
        "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator",
        "config:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/aws-control-tower" : "managed-by-control-tower"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:EnableRegion",
        "account:ListRegions",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationHooksIntegration",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:SetTypeConfiguration",
        "cloudformation:DeactivateType",
        "cloudformation:ActivateType"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:type/hook/AWS-ControlTower*"
    },
    {
      "Sid" : "AllowActionsForCloudFormationStackSetOrganizationsTrustedAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ActivateOrganizationsAccess",
        "cloudformation:DescribeOrganizationsAccess"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSCostAndUsageReportAutomationPolicy

Beschreibung: Erteilt die Berechtigung, die Organisation des Kontos zu beschreiben, S3-Buckets für das MAP-Programm zu erstellen und Tags darauf anzuwenden, einen Kosten- und Nutzungsbericht zu erstellen und Definitionen von Kosten- und Nutzungsberichten zu beschreiben.

`AWSCostAndUsageReportAutomationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSCostAndUsageReportAutomationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. November 2021, 21:27 UTC
- Zeit bearbeitet: 1. November 2021, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSCostAndUsageReportAutomationPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketTagging",
        "s3:PutBucketTagging",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:CreateBucket"
      ],
      "Resource" : "arn:aws:s3:::aws-map-cur-bucket-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions"
      ],
      "Resource" : "arn:aws:cur:*:*:definition/map-migrated-report"
    },
    {
      "Effect" : "Allow",
      "Action" : "cur:DescribeReportDefinitions",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeDataGrantOwnerFullAccess

Beschreibung: Ermöglicht Data Grant-Besitzern mithilfe des SDK AWS-Managementkonsole und den Zugriff auf AWS Data Exchange Exchange-Aktionen.

`AWSDataExchangeDataGrantOwnerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeDataGrantOwnerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Oktober 2024, 14:43 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 14:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantOwnerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:UpdateDataSet",
        "dataexchange:GetDataSet",
        "dataexchange:DeleteDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:CreateRevision",
        "dataexchange:UpdateRevision",
        "dataexchange:GetRevision",
        "dataexchange:DeleteRevision",
        "dataexchange:RevokeRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:CreateAsset",
        "dataexchange:UpdateAsset",
        "dataexchange:GetAsset",
        "dataexchange:DeleteAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset",
        "dataexchange:CreateDataGrant",
        "dataexchange:GetDataGrant",
        "dataexchange:DeleteDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:PublishToDataGrant",
        "dataexchange:SendDataSetNotification",
        "dataexchange:TagResource",
        "dataexchange:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
```

```
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES",
            "IMPORT_ASSETS_FROM_LAKE_FORMATION_TAG_POLICY"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeDataGrantReceiverFullAccess

Beschreibung: Ermöglicht dem Data Grant-Empfänger mithilfe des AWS-Managementkonsole SDK Zugriff auf AWS Data Exchange Exchange-Aktionen.

`AWSDataExchangeDataGrantReceiverFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeDataGrantReceiverFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Oktober 2024, 14:45 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 14:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeDataGrantReceiverFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet",
        "dataexchange:ListDataSets",
        "dataexchange:GetRevision",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:GetAsset",
        "dataexchange:ListRevisionAssets",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
```

```
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:GetEventAction",
        "dataexchange:ListEventActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeDataGrantActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:AcceptDataGrant",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:GetReceivedDataGrant"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des AWS-Managementkonsole SDK. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 24. Juni 2024, 19:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceProviderActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
```

```
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings",
        "aws-marketplace:DescribeAgreement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeProviderFullAccess

Beschreibung: Gewährt Datenanbietern Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS-Managementkonsole und. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeProviderFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeProviderFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 15. August 2024, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeProviderFullAccess`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateDataSet",
        "dataexchange:CreateRevision",
        "dataexchange:CreateAsset",
        "dataexchange:Get*",
        "dataexchange:Update*",
        "dataexchange:List*",
        "dataexchange:Delete*",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
        "dataexchange:PublishDataSet",
        "dataexchange:SendApiAsset",
        "dataexchange:RevokeRevision",
        "dataexchange:SendDataSetNotification",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeJobsActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "dataexchange:JobType" : [
            "IMPORT_ASSETS_FROM_S3",
            "IMPORT_ASSET_FROM_SIGNED_URL",
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "IMPORT_ASSET_FROM_API_GATEWAY_API",
            "IMPORT_ASSETS_FROM_REDSHIFT_DATA_SHARES"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3GetActionConditionalTagAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/AWSDataExchange" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3WriteActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:UpdateAgreementApprovalRequest",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftConditionalActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "redshift:ConsumerIdentifier" : "ADX"
        }
      }
    },
    {
      "Sid" : "RedshiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift:DescribeDataSharesForProducer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayActions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeReadOnly

Beschreibung: Gewährt schreibgeschützten Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS-Managementkonsole und.

`AWSDataExchangeReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetAsset",
        "dataexchange:GetDataSet",
        "dataexchange:GetEventAction",
        "dataexchange:GetJob",
        "dataexchange:GetRevision",
        "dataexchange:GetDataGrant",
        "dataexchange:GetReceivedDataGrant",
        "dataexchange:ListDataGrants",
        "dataexchange:ListReceivedDataGrants",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListDataSets",
        "dataexchange:ListEventActions",
        "dataexchange:ListJobs",
        "dataexchange:ListRevisionAssets",
        "dataexchange:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:GetAgreementTerms",
        "aws-marketplace:ListPrivateListings",
```

```
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeServiceRolePolicyForLicenseManagement

Beschreibung: Ermöglicht AWS Data Exchange den Zugriff auf AWS-Services Ressourcen, die von AWS Data Exchange für die Lizenzverwaltung verwendet oder verwaltet werden.

`AWSDataExchangeServiceRolePolicyForLicenseManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Oktober 2024, 14:54 UTC
- Bearbeitete Zeit: 10. Oktober 2024, 14:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForLicenseManagement`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeServiceRolePolicyForOrganizationDiscovery

Beschreibung: Ermöglicht AWS Data Exchange, Daten über Ihre AWS Organisation zu lesen, um festzustellen, ob Sie für die Verteilung von AWS Data Exchange Exchange-Datenzuschüssen in Frage kommen.

`AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Oktober 2024, 14:33 UTC
- Bearbeitete Zeit: 10. Oktober 2024, 14:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataExchangeServiceRolePolicyForOrganizationDiscovery`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAWSOrganizationsActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataExchangeSubscriberFullAccess

Beschreibung: Gewährt Datenabonnenten Zugriff auf AWS Data Exchange und AWS Marketplace Aktionen mithilfe des SDK AWS-Managementkonsole und. Es bietet auch ausgewählten Zugriff auf verwandte Dienste, die erforderlich sind, um den AWS Data Exchange in vollem Umfang nutzen zu können.

`AWSDataExchangeSubscriberFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataExchangeSubscriberFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2019, 19:27 UTC
- Bearbeitete Zeit: 21. Mai 2024, 17:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataExchangeSubscriberFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataExchangeReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:Get*",
        "dataexchange:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataExchangeExportActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:CancelJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dataexchange:JobType" : [
            "EXPORT_ASSETS_TO_S3",
            "EXPORT_ASSET_TO_SIGNED_URL",
            "EXPORT_REVISIONS_TO_S3"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DataExchangeEventActionActions",
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:CreateEventAction",
        "dataexchange:UpdateEventAction",
        "dataexchange:DeleteEventAction",
        "dataexchange:SendApiAsset"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetActionConditionalResourceAndADX",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*aws-data-exchange*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "dataexchange.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3ReadActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceSubscriberActions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListPrivateListings"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSActions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerServiceRole

Beschreibung: Stellt AWS Data Lifecycle Manager die entsprechenden Berechtigungen zur Verfügung, um Aktionen mit AWS Ressourcen zu ergreifen

`AWSDataLifecycleManagerServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataLifecycleManagerServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 6. Juli 2018, 19:34 UTC
- Bearbeitete Zeit: 16. Dezember 2024, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRole`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:EnableFastSnapshotRestores",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DisableFastSnapshotRestores",
        "ec2:CopySnapshot",
        "ec2:ModifySnapshotAttribute",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:ModifySnapshotTier",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:DeleteRule",
        "events:DescribeRule",
        "events:EnableRule",
        "events:DisableRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerServiceRoleForAMIManagement

Beschreibung: Stellt AWS Data Lifecycle Manager die entsprechenden Berechtigungen zur Verfügung, um Aktionen an AWS Ressourcen für AMI Management durchzuführen

`AWSDataLifecycleManagerServiceRoleForAMIManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataLifecycleManagerServiceRoleForAMIManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 21. Oktober 2020, 19:39 UTC
- Bearbeitete Zeit: 19. August 2021, 17:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerServiceRoleForAMIManagement`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImageDeprecation",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataLifecycleManagerSSMFullAccess

Beschreibung: Erlaubt Amazon Data Lifecycle Manager die Erlaubnis, die Systems Manager Manager-Aktionen auszuführen, die für die Ausführung von Pre- und Post-Skripten auf allen EC2 Amazon-Instances erforderlich sind.

`AWSDataLifecycleManagerSSMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataLifecycleManagerSSMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 31. Oktober 2023, 20:29 UTC
- Bearbeitete Zeit: 16. November 2023, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDataLifecycleManagerSSMFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTaggedSSMDocumentsOnly",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/DLMScriptsAccess" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSpecificAWSOwnedSSMDocuments",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA"
      ]
    },
    {
      "Sid" : "AllowAllEC2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataPipeline_FullAccess

Beschreibung: Bietet vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen.

`AWSDataPipeline_FullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSDataPipeline_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Januar 2017, 23:14 Uhr UTC
- Zeit bearbeitet: 17. August 2017, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "sns:Subscribe",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataPipeline_PowerUser

Beschreibung: Bietet vollen Zugriff auf Data Pipeline, Listenzugriff für S3-, DynamoDB-, Redshift-, RDS-, SNS- und IAM-Rollen sowie PassRole-Zugriff für Standardrollen.

`AWSDataPipeline_PowerUser`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSDataPipeline_PowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Januar 2017, 23:16 UTC
- Zeit bearbeitet: 17. August 2017, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataPipeline_PowerUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "s3:List*",
        "dynamodb:DescribeTable",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSecurityGroups",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSecurityGroups",
        "sns:ListTopics",
        "iam:ListRoles",
        "iam:GetRolePolicy",
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfiles",
        "datapipeline:*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/DataPipelineDefaultRole"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncDiscoveryServiceRolePolicy

Beschreibung: Ermöglicht DataSync Discovery die Integration mit anderen AWS Diensten in Ihrem Namen.

`AWSDataSyncDiscoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. März 2023, 22:19 UTC
- Bearbeitete Zeit: 20. März 2023, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncDiscoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncFullAccess

Beschreibung: Bietet vollen AWS DataSync und minimalen Zugriff auf die zugehörigen Abhängigkeiten

`AWSDataSyncFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataSyncFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 19:40 Uhr UTC
- Bearbeitete Zeit: 20. Mai 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datasync:*",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataSyncPassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datasync.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "DataSyncCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/datasync.amazonaws.com/
AWSServiceRoleForDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "datasync.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataSyncSecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS DataSync

`AWSDataSyncReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDataSyncReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Januar 2019, 19:18 UTC
- Bearbeitete Zeit: 30. Juni 2020, 17:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDataSyncReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "datasync:Describe*",
        "datasync:List*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDataSyncServiceRolePolicy

Beschreibung: Ermöglicht DataSync die Integration mit anderen AWS Diensten in Ihrem Namen

`AWSDataSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Oktober 2024, 17:45 UTC
- Bearbeitete Zeit: 15. April 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataSyncCloudWatchLogCreateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*"
      ]
    },
    {
      "Sid" : "DataSyncCloudWatchLogStreamUpdateAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:*:logs:*:*:log-group:/aws/datasync*:log-stream:*"
      ]
    },
    {
      "Sid" : "DataSyncSecretsManagerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:*:secretsmanager:*:*:secret:aws-datasync!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "aws-
datasync",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-FleetWorker

Beschreibung: Ermöglicht Mitarbeitern von AWS Deadline Cloud den Zugriff auf die Ausführung von Aufgaben auf einer Farm.

`AWSDeadlineCloud-FleetWorker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-FleetWorker` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:21 UTC
- Bearbeitete Zeit: 1. April 2024, 17:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RunTasksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForWorker",
        "deadline:UpdateWorker",
        "deadline:UpdateWorkerSchedule",
```

```
        "deadline:BatchGetJobEntity",
        "deadline:AssumeQueueRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessFarms

Beschreibung: Ermöglicht Benutzern Workstation-Zugriff auf AWS Deadline Cloud-Farmen mit eingeschränkten Leseberechtigungen, um andere erforderliche Dienste aufzurufen. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessFarms`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-UserAccessFarms` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 16:54 UTC
- Bearbeitete Zeit: 7. Oktober 2024, 17:57 UTC

- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFarms`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:CreateBudget",
        "deadline:DeleteBudget",
        "deadline:DisassociateMemberFromFarm",
```

```
        "deadline:DisassociateMemberFromFleet",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue",
        "deadline:GetBudget",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:ListBudgets",
        "deadline:StartSessionsStatisticsAggregation",
        "deadline:UpdateBudget"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFarm",
        "deadline:AssociateMemberToFleet",
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
```

```
        ],
        "deadline:MembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER"
        ]
      }
    }
  },
  {
    "Sid" : "ManagerLevelMemberDisassociation",
    "Effect" : "Allow",
    "Action" : [
      "deadline:DisassociateMemberFromFarm",
      "deadline:DisassociateMemberFromFleet",
      "deadline:DisassociateMemberFromJob",
      "deadline:DisassociateMemberFromQueue"
    ],
    "Resource" : [
      "*"
    ],
    "Condition" : {
      "ForAnyValue:StringEquals" : {
        "deadline:FarmMembershipLevels" : [
          "MANAGER"
        ]
      },
      "StringEquals" : {
        "deadline:AssociatedMembershipLevel" : [
          "MANAGER",
          "CONTRIBUTOR",
          "VIEWER",
          ""
        ]
      }
    }
  },
  {
    "Sid" : "OwnerManagerPermissions",
    "Effect" : "Allow",
    "Action" : [
      "deadline:ListFarmMembers",
      "deadline:ListFleetMembers",
      "deadline:ListJobMembers",
```

```
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:AssumeQueueRoleForRead",
```

```
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FarmMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFarms",
        "deadline:ListFleets",
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessFleets

Beschreibung: Ermöglicht Benutzern den Workstation-Zugriff auf AWS Deadline Cloud-Flotten mit eingeschränkten Leseberechtigungen, um andere erforderliche Dienste aufzurufen. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessFleets`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-UserAccessFleets` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:01 UTC
- Bearbeitete Zeit: 1. April 2024, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessFleets`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
```

```
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet",
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
```

```
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleetMembers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeFleetRoleForRead",
        "deadline:GetFleet",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetWorker",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionsForWorker",
        "deadline:ListWorkers",
        "deadline:SearchWorkers"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:FleetMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListFleets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessJobs

Beschreibung: Ermöglicht Benutzern Workstation-Zugriff auf AWS Deadline Cloud-Jobs mit eingeschränkten Leseberechtigungen zum Aufrufen anderer erforderlicher Dienste. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessJobs`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-UserAccessJobs` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:05 UTC
- Bearbeitete Zeit: 7. Oktober 2024, 18:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessJobs`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "MANAGER"
          ]
```

```
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
```

```
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListTasks",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:JobMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-UserAccessQueues

Beschreibung: Ermöglicht Benutzerarbeitsstationen den Zugriff auf AWS Deadline Cloud-Warteschlangen mit eingeschränkten Leseberechtigungen zum Aufrufen anderer erforderlicher Dienste. Ordnen Sie diese Richtlinie der Benutzerrolle zu, die Ihrem Studio zugeordnet ist.

`AWSDeadlineCloud-UserAccessQueues`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-UserAccessQueues` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:10 UTC
- Bearbeitungszeit: 7. Oktober 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-UserAccessQueues`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AdditionalPermissions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:ListGroupMembershipsForMember",
        "deadline:GetApplicationVersion",
        "ec2:DescribeInstanceTypes",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OwnerLevelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue",
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberAssociation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "deadline:AssociateMemberToJob",
        "deadline:AssociateMemberToQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ],
          "deadline:MembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ManagerLevelMemberDisassociation",
      "Effect" : "Allow",
      "Action" : [
        "deadline:DisassociateMemberFromJob",
        "deadline:DisassociateMemberFromQueue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "MANAGER"
          ]
        },
```

```
        "StringEquals" : {
          "deadline:AssociatedMembershipLevel" : [
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER",
            ""
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobMembers",
        "deadline:ListQueueMembers",
        "deadline:UpdateJob",
        "deadline:UpdateSession",
        "deadline:UpdateStep",
        "deadline:UpdateTask"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER"
          ]
        }
      }
    },
    {
      "Sid" : "OwnerManagerContributorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForUser",
        "deadline:CreateJob"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR"
          ]
        }
      }
    },
    {
      "Sid" : "AllLevelsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:AssumeQueueRoleForRead",
        "deadline:GetJob",
        "deadline:GetJobTemplate",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetStep",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTasks",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "deadline:QueueMembershipLevels" : [
```

```
            "OWNER",
            "MANAGER",
            "CONTRIBUTOR",
            "VIEWER"
          ]
        }
      }
    },
    {
      "Sid" : "ListBasedOnMembership",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListJobs",
        "deadline:ListQueues"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "deadline:RequesterPrincipalId" : "${deadline:PrincipalId}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeadlineCloud-WorkerHost

Beschreibung: Ermöglicht AWS Deadline Cloud-Worker-Hosts den Zugriff, um einer Flotte in einer Farm beizutreten.

`AWSDeadlineCloud-WorkerHost`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeadlineCloud-WorkerHost` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2024, 17:28 UTC
- Bearbeitete Zeit: 30. April 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "JoinFleetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "deadline:CreateWorker",
        "deadline:AssumeFleetRoleForWorker"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TagWorkerPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:TagResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*/worker/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    },
    {
      "Sid" : "ListFleetTagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "deadline:ListTagsForResource"
      ],
      "Resource" : "arn:aws:deadline:*:*:farm/*/fleet/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}",
          "deadline:CalledAction" : "CreateWorker"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepLensLambdaFunctionAccessPolicy

Beschreibung: Diese Richtlinie legt die Berechtigungen fest, die für DeepLens administrative Lambda-Funktionen erforderlich sind, die auf einem DeepLens Gerät ausgeführt werden

`AWSDeepLensLambdaFunctionAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepLensLambdaFunctionAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 15:47 Uhr UTC
- Bearbeitete Zeit: 11. Juni 2019, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepLensLambdaFunctionAccessPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::deeplens*/*",
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:DescribeStream",
        "kinesisvideo:CreateStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepLensServiceRolePolicy

Beschreibung: Gewährt AWS DeepLens Zugriff auf Ressourcen und Rollen AWS-Services, die von DeepLens und seinen Abhängigkeiten benötigt werden, einschließlich IoT, S3 GreenGrass und AWS Lambda.

`AWSDeepLensServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepLensServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. November 2017, 15:46 Uhr UTC
- Bearbeitete Zeit: 25. September 2019, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepLensServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepLensIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIoTAttachCertificatePolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/deeplens*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "DeepLensIoTDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensAccess",
      "Effect" : "Allow",
      "Action" : [
        "deeplens:*"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "DeepLensS3ObjectAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensCreateS3Buckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensIAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com",
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DeepLensIAMLambdaPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepLens*",
        "arn:aws:iam::*:role/service-role/AWSDeepLens*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DeepLensGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
```

```
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
```

```
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaAdminFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerWriteAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:StopTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/deeplens*"
      ]
    },
    {
      "Sid" : "DeepLensSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoStreamAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:DeleteStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/deeplens*/*"
      ]
    },
    {
      "Sid" : "DeepLensKinesisVideoEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:GetDataEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerAccountAdminAccess

Beschreibung: DeepRacer Administratorzugriff auf alle Aktionen, einschließlich des Umschaltens zwischen Mehrbenutzer- und Einzelbenutzermodus.

`AWSDeepRacerAccountAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerAccountAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Oktober 2021, 01:27 UTC
- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerAccountAdminAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeepRacerAdminAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerCloudFormationAccessPolicy

Beschreibung: Ermöglicht CloudFormation das Erstellen und Verwalten von AWS Stacks und Ressourcen in Ihrem Namen.

`AWSDeepRacerCloudFormationAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerCloudFormationAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 14. Juni 2019, 17:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerCloudFormationAccessPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachInternetGateway",
        "ec2:DisassociateRouteTable",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/service-role/AWSDeepRacerLambdaAccessRole",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:DeleteBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "robomaker:CreateSimulationApplication",
        "robomaker:CreateSimulationApplicationVersion",
        "robomaker:DeleteSimulationApplication",
        "robomaker:DescribeSimulationApplication",
        "robomaker:ListSimulationApplications",
        "robomaker:TagResource",
        "robomaker:UpdateSimulationApplication"
      ],
      "Resource" : [
        "arn:aws:robomaker:*:*:/createSimulationApplication",
        "arn:aws:robomaker:*:*:simulation-application/deepracer*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerDefaultMultiUserAccess

Beschreibung: DeepRacer MultiUser Standardbenutzerzugriff zur Verwendung von Deepracer im Mehrbenutzermodus

`AWSDeepRacerDefaultMultiUserAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerDefaultMultiUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. Oktober 2021, 01:27 UTC
- Bearbeitete Zeit: 28. Oktober 2021, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerDefaultMultiUserAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:Add*",
        "deepracer:Remove*",
        "deepracer:Create*",
        "deepracer:Perform*",
        "deepracer:Clone*",
        "deepracer:Get*",
        "deepracer:List*",
        "deepracer:Edit*",
        "deepracer:Start*",
        "deepracer:Set*",
        "deepracer:Update*",
        "deepracer:Delete*",
        "deepracer:Stop*",
        "deepracer:Import*",
        "deepracer:Tag*",
        "deepracer:Untag*"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "Null" : {
          "deepracer:UserToken" : "false"
        },
        "Bool" : {
          "deepracer:MultiUser" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:GetAccountConfig",
        "deepracer:GetTrack",
        "deepracer:ListTracks",
        "deepracer:TestRewardFunction"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "deepracer:Admin*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS DeepRacer. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3).

`AWSDeepRacerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Oktober 2020, 22:03 UTC
- Bearbeitete Zeit: 5. Oktober 2020, 22:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*",
        "arn:aws:s3:::*DeepRacer*/*",
        "arn:aws:s3:::*Deepracer*/*",
        "arn:aws:s3:::*deepracer*/*",
        "arn:aws:s3:::dr-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerRoboMakerAccessPolicy

Beschreibung: Ermöglicht RoboMaker das Erstellen der erforderlichen Ressourcen und das Anrufen von AWS Diensten in Ihrem Namen.

`AWSDeepRacerRoboMakerAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerRoboMakerAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. Februar 2019, 21:59 UTC
- Bearbeitete Zeit: 28. Februar 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeepRacerRoboMakerAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:CreateNetworkInterfacePermission",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs",
        "arn:aws:logs:*:*:log-group:/aws/robomaker/SimulationJobs:log-stream:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeepRacerServiceRolePolicy

Beschreibung: Ermöglicht DeepRacer das Erstellen der erforderlichen Ressourcen und das Anrufen von AWS Diensten in Ihrem Namen.

`AWSDeepRacerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeepRacerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. Februar 2019, 21:58 Uhr UTC
- Bearbeitete Zeit: 12. Juni 2019, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSDeepRacerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "deepracer:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "robomaker:*",
        "sagemaker:*",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DetectStackDrift",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackResourceDrifts"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      },
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSDeepRacer*",
        "arn:aws:iam::*:role/service-role/AWSDeepRacer*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionCode"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*DeepRacer*",
        "arn:aws:lambda:*:*:function:*Deepracer*",
        "arn:aws:lambda:*:*:function:*deepracer*",
        "arn:aws:lambda:*:*:function:*dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::*DeepRacer*",
        "arn:aws:s3:::*Deepracer*",
        "arn:aws:s3:::*deepracer*",
        "arn:aws:s3:::dr-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "s3:ExistingObjectTag/DeepRacer" : "true"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesisvideo:CreateStream",
        "kinesisvideo:DeleteStream",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:GetDataEndpoint",
        "kinesisvideo:GetHLSStreamingSessionURL",
        "kinesisvideo:GetMedia",
        "kinesisvideo:PutMedia",
        "kinesisvideo:TagStream"
      ],
      "Resource" : [
        "arn:aws:kinesisvideo:*:*:stream/dr-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDenyAll

Beschreibung: Jeglichen Zugriff verweigern.

`AWSDenyAll`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDenyAll` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Mai 2019, 22:36 UTC
- Bearbeitete Zeit: 18. Dezember 2023, 16:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDenyAll`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAll",
      "Effect" : "Deny",
      "Action" : [
        "*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Device Farm Farm-Operationen.

`AWSDeviceFarmFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDeviceFarmFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Juli 2015, 16:37 UTC
- Bearbeitete Zeit: 13. Juli 2015, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDeviceFarmFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "devicefarm:*"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmServiceRolePolicy

Beschreibung: Erteilen Sie AWS Device Farm die Erlaubnis, EC2 Network in APIs Ihrem Namen anzurufen.

`AWSDeviceFarmServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. September 2022, 21:02 UTC
- Bearbeitete Zeit: 20. September 2022, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDeviceFarmTestGridServiceRolePolicy

Beschreibung: Erteilen Sie AWS Device Farm die Erlaubnis, in EC2 APIs Ihrem Namen anzurufen.

`AWSDeviceFarmTestGridServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Mai 2021, 22:01 UTC
- Bearbeitete Zeit: 26. Mai 2021, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDeviceFarmTestGridServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSDeviceFarmManaged" : "true"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AWSDeviceFarmManaged" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Direct Connect über die AWS-Managementkonsole.

`AWSDirectConnectFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectConnectFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 30. April 2019, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Direct Connect über die AWS-Managementkonsole.

`AWSDirectConnectReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 18. Mai 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:Describe*",
        "directconnect:List*",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectConnectServiceRolePolicy

Beschreibung: AWS Erlaubt Direct Connect, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AWSDirectConnectServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. Januar 2021, 18:35 UTC
- Bearbeitete Zeit: 14. Januar 2021, 18:35 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectConnectServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*directconnect*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceDataFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Verzeichnisdienstdaten.

`AWSDirectoryServiceDataFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectoryServiceDataFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. September 2024, 21:45 Uhr UTC
- Bearbeitete Zeit: 18. September 2024, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:AddGroupMember",
        "ds-data:CreateGroup",
        "ds-data:CreateUser",
        "ds-data:DeleteGroup",
        "ds-data:DeleteUser",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:DisableUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:RemoveGroupMember",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers",
        "ds-data:UpdateGroup",
        "ds-data:UpdateUser"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceDataReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Verzeichnisdienstdaten

`AWSDirectoryServiceDataReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectoryServiceDataReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. September 2024, 22:00 Uhr UTC
- Bearbeitete Zeit: 18. September 2024, 22:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceDataReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSDataReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:AccessDSData",
        "ds-data:DescribeGroup",
        "ds-data:DescribeUser",
        "ds-data:ListGroupMembers",
        "ds-data:ListGroups",
        "ds-data:ListGroupsForMember",
        "ds-data:ListUsers",
        "ds-data:SearchGroups",
        "ds-data:SearchUsers"
      ],
      "Resource" : [
        "arn:aws:ds:*:*:directory/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Directory Service.

`AWSDirectoryServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectoryServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 02. April 2024, 20:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DirectoryServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ds:*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
```

```
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "iam:ListRoles",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DirectoryServiceEventTopic",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:DirectoryMonitoring*"
    },
    {
      "Sid" : "DirectoryServiceOrganizations",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ds.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "DirectoryServiceTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Directory Service.

`AWSDirectoryServiceReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDirectoryServiceReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 25. September 2018, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDirectoryServiceReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDirectoryServiceServiceRolePolicy

Beschreibung: Richtlinie für die verknüpfte Verzeichnisdienst-Rolle

`AWSDirectoryServiceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Juli 2025, 00:22 UTC
- Bearbeitungszeit: 11. Juli 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDirectoryServiceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "EC2DescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "ssm:GetConnectionStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDiscoveryContinuousExportFirehosePolicy

Beschreibung: Bietet Schreibzugriff auf AWS Ressourcen, die für AWS Discovery Continuous Export erforderlich sind

`AWSDiscoveryContinuousExportFirehosePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSDiscoveryContinuousExportFirehosePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. August 2018, 18:29 Uhr UTC
- Bearbeitete Zeit: 8. Juni 2021, 17:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSDiscoveryContinuousExportFirehosePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-application-discovery-service-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/firehose:log-
stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDMSFleetAdvisorServiceRolePolicy

Beschreibung: Ermöglicht DMS Fleet Advisor, CloudWatch Metriken in Ihrem Namen zu verwalten.

`AWSDMSFleetAdvisorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. März 2023, 09:10 UTC
- Bearbeitete Zeit: 6. März 2023, 09:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSFleetAdvisorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "cloudwatch:PutMetricData",
    "Resource" : "*",
    "Condition" : {
```

```
      "StringEquals" : {
        "cloudwatch:namespace" : "AWS/DMS/FleetAdvisor"
      }
    }
  }
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSDMSServerlessServiceRolePolicy

Beschreibung: Erteilt AWS DMS Serverless die Berechtigung, in Ihrem Namen DMS-Ressourcen in Ihrem Konto zu erstellen und zu verwalten

`AWSDMSServerlessServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Mai 2023, 20:28 UTC
- Zeit bearbeitet: 5. November 2025, 14:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSDMSServerlessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "id0",
      "Effect" : "Allow",
      "Action" : [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "dms:req-tag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id1",
      "Effect" : "Allow",
      "Action" : [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "id2",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms:ModifyReplicationTask",
        "dms:DeleteReplicationTask",
        "dms:ModifyReplicationInstance",
        "dms:DeleteReplicationInstance"
```

```
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "aws:ResourceTag/ResourceCreatedBy" : "DMSServerless"
        }
      }
    },
    {
      "Sid" : "id3",
      "Effect" : "Allow",
      "Action" : [
        "dms:TestConnection",
        "dms:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:endpoint:*"
      ]
    },
    {
      "Sid" : "id4",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id5",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::dms-serverless-premigration-results-*",
        "arn:aws:s3:::dms-premigration-results-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "id6",
      "Effect" : "Allow",
      "Action" : [
        "dms:StartReplicationTaskAssessmentRun"
      ],
      "Resource" : [
        "arn:aws:dms:*:*:task:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2CapacityManagerServiceRolePolicy

Beschreibung: Ermöglicht EC2 Capacity Manager, Kapazitätsressourcen zu verwalten und in Ihrem Namen in AWS Organizations zu integrieren.

`AWSEC2CapacityManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Oktober 2025, 22:04 UTC
- Bearbeitete Zeit: 9. Oktober 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOrganizationsDefaultReadActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsListDelegatedAdministratorsAction",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "ec2.capacitymanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2CapacityReservationFleetRolePolicy

Beschreibung: Ermöglicht dem EC2 CapacityReservation Flottenservice die Verwaltung von Kapazitätsreservierungen

`AWSEC2CapacityReservationFleetRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. September 2021, 14:43 UTC
- Bearbeitete Zeit: 03. März 2025, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2CapacityReservationFleetRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateCapacityReservation",
        "ec2:CancelCapacityReservation",
        "ec2:ModifyCapacityReservation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:CapacityReservationFleet" : "arn:aws:ec2:*:*:capacity-reservation-fleet/
crf-*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateCapacityReservation"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2FleetServiceRolePolicy

Beschreibung: Ermöglicht EC2 Fleet, Instanzen zu starten und zu verwalten.

`AWSEC2FleetServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. März 2018, 00:08 Uhr UTC
- Bearbeitete Zeit: 4. Mai 2020, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2FleetServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "EC2SpotManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "spot.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SpotFleetServiceRolePolicy

Beschreibung: Ermöglicht EC2 Spot Fleet, Spot-Flotteninstanzen zu starten und zu verwalten

`AWSEC2SpotFleetServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Oktober 2017, 19:13 Uhr UTC
- Bearbeitete Zeit: 16. März 2020, 19:16 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotFleetServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:RequestSpotInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*",
        "arn:aws:ec2:*:*:spot-fleet-request/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SpotServiceRolePolicy

Beschreibung: Ermöglicht EC2 Spot das Starten und Verwalten von Spot-Instances

`AWSEC2SpotServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 18. September 2017, 18:51 Uhr UTC
- Bearbeitete Zeit: 12. Dezember 2018, 00:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SpotServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
```

```
          "ec2:InstanceMarketType" : "spot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SqlHaInstancePolicy

Beschreibung: EC2 Amazon-Instance-Berechtigungen, die es dem EC2 SQL High Availability Service ermöglichen, den Hochverfügbarkeitsstatus der EC2 Instance anhand des Instance-Profils zu erkennen.

`AWSEC2SqlHaInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSEC2SqlHaInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2025, 01:49 UTC
- Zeit bearbeitet: 13. November 2025, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2SqlHaInstancePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateInstanceInformation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
```

```
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/AWSEc2SqlHa" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2messages:AcknowledgeMessage",
        "ec2messages:DeleteMessage",
        "ec2messages:FailMessage",
        "ec2messages:GetEndpoint",
        "ec2messages:GetMessages",
        "ec2messages:SendReply"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2SqlHaServiceRolePolicy

Beschreibung: EC2 SQL High Availability-Dienstberechtigungen zur Erkennung von standby/passive Instanzen

`AWSEC2SqlHaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2025, 01:34 UTC
- Zeit bearbeitet: 13. November 2025, 01:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEC2SqlHaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSSMSendCommandToTaggedInstances",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SqlHaMonitored" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendCommandOfOwnedDoc",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSEC2-DetectSqlHa*"
      ]
    },
    {
      "Sid" : "AllowSSMNonMutating",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2NonMutating",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEventsMutateManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:PutRule",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2sqlha.amazonaws.com",
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    },
    {
      "Sid" : "AllowEventsNonMutatingManagedRule",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AWSEC2SqlHa*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEC2VssSnapshotPolicy

Beschreibung: Diese Richtlinie ist an die IAM-Rolle angehängt, die Ihren Amazon EC2 Windows-Instances zugewiesen ist, damit die Amazon EC2 VSS-Lösung Tags erstellen und Amazon Machine Images (AMI) und EBS-Snapshots hinzufügen kann.

`AWSEC2VssSnapshotPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSEC2VssSnapshotPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2024, 16:32 UTC
- Bearbeitete Zeit: 20. November 2024, 17:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEC2VssSnapshotPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeInstanceInfo",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotsAccessVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshots"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Sid" : "CreateImageWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AwsVssConfig" : "*"
        }
      }
    },
    {
      "Sid" : "CreateImageAccessInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateImage"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:SourceInstanceARN" : "arn:aws:ec2:*:*:instance/${ec2:InstanceId}"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateImage",
            "CreateSnapshots"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsAfterResourceCreation",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/AwsVssConfig" : "*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AppConsistent",
            "Device"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeImagesAndSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSECRPullThroughCache_ServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die vom AWS ECR-Pull-Through-Cache verwendet oder verwaltet werden

`AWSECRPullThroughCache_ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2021, 21:51 UTC
- Bearbeitete Zeit: 06. März 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSECRPullThroughCache_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECR",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken",
        "ecr:BatchCheckLayerAvailability",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:PutImage",
        "ecr:BatchGetImage",
        "ecr:BatchImportUpstreamImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetImageCopyStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:ecr-pullthroughcache/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkCustomPlatformforEC2Role

Beschreibung: Erteilen Sie der Instance in Ihrer benutzerdefinierten Platform Builder-Umgebung die Berechtigung, EC2 Instance zu starten, EBS-Snapshot und AMI zu erstellen, Logs an Amazon CloudWatch Logs zu streamen und Artefakte in Amazon S3 zu speichern.

`AWSElasticBeanstalkCustomPlatformforEC2Role`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkCustomPlatformforEC2Role` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Februar 2017, 22:50 UTC
- Zeit bearbeitet: 21. Februar 2017, 22:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkCustomPlatformforEC2Role`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "EC2Access",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeypair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DeleteKeypair",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSnapshot",
        "ec2:DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DetachVolume",
        "ec2:GetPasswordData",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySnapshotAttribute",
        "ec2:RegisterImage",
        "ec2:RunInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/platform/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkEnhancedHealth

Beschreibung: AWS Elastic Beanstalk Service-Richtlinie für das Gesundheitsüberwachungssystem

`AWSElasticBeanstalkEnhancedHealth`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkEnhancedHealth` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Februar 2016, 23:17 UTC
- Bearbeitete Zeit: 9. April 2018, 22:12 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkEnhancedHealth`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:GetConsoleOutput",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeSecurityGroups",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
```

```
        "autoscaling:DescribeNotificationConfigurations",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*:log-stream:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkMaintenance

Beschreibung: AWS Elastic Beanstalk Service Role Policy, die eingeschränkte Berechtigungen zur Aktualisierung Ihrer Ressourcen in Ihrem Namen zu Wartungszwecken gewährt.

`AWSElasticBeanstalkMaintenance`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Januar 2019, 23:22 UTC
- Bearbeitete Zeit: 29. April 2024, 21:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkMaintenance`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationChangeSetOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStacks",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
```

```
    },
    {
      "Sid" : "AllowElasticBeanstalkStacksUpdateExecuteSuccessfully",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy

Beschreibung: Diese Richtlinie gilt für die AWS Elastic Beanstalk-Servicerolle, die zur Durchführung verwalteter Updates von Elastic Beanstalk Beanstalk-Umgebungen verwendet wird. Diese Richtlinie sollte nicht mit anderen Benutzern oder Rollen verknüpft werden. Die Richtlinie gewährt umfassende Berechtigungen zum Erstellen und Verwalten von Ressourcen für eine Reihe von AWS Diensten AutoScaling, darunter ECS EC2, Elastic Load Balancing und CloudFormation. Diese Richtlinie ermöglicht auch die Weitergabe jeder IAM-Rolle, die mit diesen Diensten verwendet werden kann.

`AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. März 2021, 22:18 Uhr UTC
- Bearbeitete Zeit: 27. Februar 2025, 16:07 UTC

- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkManagedUpdatesCustomerRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElasticBeanstalkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "EC2BroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteSecurityGroup",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2RunInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "EC2TerminateInstancesOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ECSBroadOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECSDeleteClusterOperationPermissions",
      "Effect" : "Allow",
      "Action" : "ecs:DeleteCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/awseb-*"
    },
    {
      "Sid" : "ASGOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
```

```
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFNOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "ELBOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DeregisterTargets",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*/eb-*/*"
      ]
    },
    {
      "Sid" : "CWLogsOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "S3ObjectOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3BucketOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "SNSOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:SetTopicAttributes",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
    },
    {
      "Sid" : "SQSOperationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:awseb-e-*",
        "arn:aws:sqs:*:*:eb-*"
      ]
    },
    {
      "Sid" : "CWPutMetricAlarmOperationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:awseb-*",
        "arn:aws:cloudwatch:*:*:alarm:eb-*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchTemplateTagPropagationPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:createTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "RunInstances"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkManagedUpdatesServiceRolePolicy

Beschreibung: AWS Elastic Beanstalk Service Role-Richtlinie, die eingeschränkte Berechtigungen für verwaltete Updates gewährt.

`AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. November 2019, 22:35 Uhr UTC
- Bearbeitete Zeit: 29. April 2024, 23:11 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkManagedUpdatesServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPassRoleToElasticBeanstalkAndDownstreamServices",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SingleInstanceAPIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:releaseAddress",
        "ec2:allocateAddress",
        "ec2:DisassociateAddress",
```

```
        "ec2:AssociateAddress"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition",
        "ecs:List*",
        "ecs:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElasticBeanstalkAPIs",
      "Effect" : "Allow",
      "Action" : [
        "elasticbeanstalk:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyAPIs",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:Describe*",
        "cloudformation:List*",
        "ec2:Describe*",
        "autoscaling:Describe*",
        "elasticloadbalancing:Describe*",
        "logs:DescribeLogGroups",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
```

```
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*",
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/eb-*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/eb-*"
      ]
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CancelUpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-e-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" : [
            "arn:aws:cloudformation:*:*:stack/awseb-e-*",
            "arn:aws:cloudformation:*:*:stack/eb-*"
          ]
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*/*"
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-e-*",
        "arn:aws:elasticloadbalancing:*:*:targetgroup/eb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/eb-*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ElasticBeanstalkNotifications-Environment-*"
    },
    {
      "Sid" : "EC2LaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*"
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkMulticontainerDocker

Beschreibung: Gewähren Sie den Instances in Ihrer Docker-Umgebung mit mehreren Containern Zugriff, um den Amazon EC2 Container Service zur Verwaltung von Container-Bereitstellungsaufgaben zu verwenden.

`AWSElasticBeanstalkMulticontainerDocker`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkMulticontainerDocker` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:15 UTC
- Bearbeitete Zeit: 23. März 2023, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkMulticontainerDocker`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ECSAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecs:Poll",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DiscoverPollEndpoint",
        "ecs:StartTelemetrySession",
        "ecs:RegisterContainerInstance",
        "ecs:DeregisterContainerInstance",
        "ecs:DescribeContainerInstances",
```

```
        "ecs:Submit*",
        "ecs:DescribeTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "RegisterContainerInstance",
            "StartTask"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkReadOnly

Beschreibung: Gewährt nur Leseberechtigungen. Ermöglicht Betreibern ausdrücklich den direkten Zugriff auf Informationen über Ressourcen im Zusammenhang mit AWS Elastic Beanstalk Beanstalk-Anwendungen.

`AWSElasticBeanstalkReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Januar 2021, 19:02 UTC
- Bearbeitete Zeit: 22. Januar 2021, 19:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAPIs",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudtrail:LookupEvents",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfiles",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListServerCertificates",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
```

```
        "rds:DescribeDBSnapshots",
        "s3:ListAllMyBuckets",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleCore

Beschreibung: AWSElastic BeanstalkRoleCore (Rolle „Elastic Beanstalk Operations“) Ermöglicht den Kernbetrieb einer Webservice-Umgebung.

`AWSElasticBeanstalkRoleCore`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleCore` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:48 UTC
- Bearbeitete Zeit: 30. April 2024, 00:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCore`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/awseb-e-*"
        }
      }
    },
    {
```

```
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReleaseAddress",
        "ec2:AllocateAddress",
        "ec2:DisassociateAddress",
        "ec2:AssociateAddress",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroup*",
        "ec2:RevokeSecurityGroup*",
        "ec2:CreateLaunchTemplate*",
        "ec2:DeleteLaunchTemplate*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LTRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "ASG",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:*LoadBalancer*",
        "autoscaling:*AutoScalingGroup",
        "autoscaling:*LaunchConfiguration",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DetachInstances",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses",
```

```
        "autoscaling:*Tags"
      ],
      "Resource" : [
        "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/awseb-e-
*",
        "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/awseb-e-*"
      ]
    },
    {
      "Sid" : "ASGPolicy",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DeletePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EBSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/elasticbeanstalk.amazonaws.com/
AWSServiceRoleForElasticBeanstalk*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticbeanstalk.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3Obj",
      "Effect" : "Allow",
      "Action" : [
        "s3:Delete*",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*/*",
```

```
        "arn:aws:s3:::elasticbeanstalk-env-resources-*/*"
      ]
    },
    {
      "Sid" : "S3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucket*",
        "s3:ListBucket",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Sid" : "CFN",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CancelUpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awseb-e-*"
    },
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:awseb-*"
    },
    {
      "Sid" : "ELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Create*",
        "elasticloadbalancing:Delete*",
```

```
        "elasticloadbalancing:Modify*",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeRegisterTargets",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:*Tags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:SetRulePriorities",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:targetgroup/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/net/awseb-*/*",
        "arn:aws:elasticloadbalancing:*:*:listener/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/app/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener/net/awseb-*",
        "arn:aws:elasticloadbalancing:*:*:listener-rule/app/awseb-*/*/*/*"
      ]
    },
    {
      "Sid" : "ListAPIs",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudformation:Describe*",
        "logs:Describe*",
        "ec2:Describe*",
        "ecs:Describe*",
        "ecs:List*",
        "elasticloadbalancing:Describe*",
        "rds:Describe*",
        "sns:List*",
        "iam:List*",
        "acm:Describe*",
        "acm:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-elasticbeanstalk-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticbeanstalk.amazonaws.com",
            "ec2.amazonaws.com",
            "autoscaling.amazonaws.com",
            "elasticloadbalancing.amazonaws.com",
            "ecs.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleCWL

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung die Verwaltung von Amazon CloudWatch Logs-Protokollgruppen.

`AWSElasticBeanstalkRoleCWL`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleCWL` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 5. Juni 2020, 21:49 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleCWL`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleECS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Docker-Umgebung mit mehreren Containern die Verwaltung von Amazon ECS-Clustern.

`AWSElasticBeanstalkRoleECS`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleECS` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:47 UTC
- Bearbeitete Zeit: 23. März 2023, 22:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleECS`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
```

```
        "ecs:RegisterTaskDefinition",
        "ecs:DeRegisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleRDS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung die Integration einer Amazon RDS-Instance.

`AWSElasticBeanstalkRoleRDS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleRDS` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:46 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleRDS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBSecurityGroup",
        "rds:DeleteDBSecurityGroup",
        "rds:AuthorizeDBSecurityGroupIngress",
        "rds:CreateDBInstance",
        "rds:ModifyDBInstance",
        "rds:DeleteDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:secgrp:awseb-e-*",
        "arn:aws:rds:*:*:db:*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleSNS

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Umgebung, die Amazon SNS SNS-Themenintegration zu ermöglichen.

`AWSElasticBeanstalkRoleSNS`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleSNS` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:46 Uhr UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:46 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleSNS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowBeanstalkManageSNS",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:SetTopicAttributes",
        "sns:DeleteTopic"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:ElasticBeanstalkNotifications-*"
      ]
    },
    {
      "Sid" : "AllowSNSPublish",
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkRoleWorkerTier

Beschreibung: (Rolle „Elastic Beanstalk Operations“) Ermöglicht einer Worker-Umgebungsebene, eine Amazon DynamoDB-Tabelle und eine Amazon SQS SQS-Warteschlange zu erstellen.

`AWSElasticBeanstalkRoleWorkerTier`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkRoleWorkerTier` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2020, 21:43 UTC
- Bearbeitete Zeit: 5. Juni 2020, 21:43 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkRoleWorkerTier`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:TagQueue",
```

```
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
      ],
      "Resource" : "arn:aws:sqs:*:*:awseb-e-*"
    },
    {
      "Sid" : "AllowDDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:DeleteTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awseb-e-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkService

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https:// docs.aws.amazon.com/elasticbeanstalk/ latest/dg/iam -servicerole.html. AWS Elastic Beanstalk Service-Rollenrichtlinie, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.: AutoScaling, EC2, S3, CloudFormation, ELB usw.) in Ihrem Namen gewährt.

`AWSElasticBeanstalkService`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkService` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. April 2016, 20:27 UTC
- Bearbeitete Zeit: 10. Mai 2023, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticBeanstalkService`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowDeleteCloudwatchLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
```

```
      ]
    },
    {
      "Sid" : "AllowECSTagResource",
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : [
            "CreateCluster",
            "RegisterTaskDefinition"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3OperationsOnElasticBeanstalkBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:*"
      ],
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "AllowLaunchTemplateRunInstances",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:LaunchTemplate" : "arn:aws:ec2:*:*:launch-template/*"
        }
      }
    },
    {
      "Sid" : "AllowELBAddTags",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:AddTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "elasticloadbalancing:CreateAction" : [
            "CreateLoadBalancer"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:AttachInstances",
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteLaunchConfiguration",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:DeleteScheduledAction",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:DescribeScheduledActions",
        "autoscaling:DetachInstances",
        "autoscaling:DeletePolicy",
        "autoscaling:PutScalingPolicy",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:ResumeProcesses",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:SuspendProcesses",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "cloudwatch:PutMetricAlarm",
        "ec2:AssociateAddress",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeVpcClassicLink",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:TerminateInstances",
        "ecs:CreateCluster",
        "ecs:DeleteCluster",
        "ecs:DescribeClusters",
        "ecs:RegisterTaskDefinition",
        "elasticbeanstalk:*",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancer",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets",
        "iam:ListRoles",
```

```
        "iam:PassRole",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogGroups",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeOrderableDBInstanceOptions",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:ListBucket",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:SetTopicAttributes",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:BatchGetBuilds",
        "codebuild:StartBuild"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkServiceRolePolicy

Beschreibung: AWS Elastic Beanstalk Service Linked Role-Richtlinie, die Berechtigungen zum Erstellen und Verwalten von Ressourcen (d. h.: AutoScaling, EC2, S3, CloudFormation, ELB usw.) in Ihrem Namen gewährt.

`AWSElasticBeanstalkServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. September 2017, 23:46 Uhr UTC
- Bearbeitete Zeit: 6. Juni 2019, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticBeanstalkServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCloudformationReadOperationsOnElasticBeanstalkStacks",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/awseb-*",
        "arn:aws:cloudformation:*:*:stack/eb-*"
      ]
    },
    {
      "Sid" : "AllowOperations",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribeScalingActivities",
        "autoscaling:PutNotificationConfiguration",
        "ec2:DescribeInstanceStatus",
        "ec2:AssociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "lambda:GetFunction",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOperationsOnHealthStreamingLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
```

```
        "logs:DeleteLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkWebTier

Beschreibung: Geben Sie den Instances in Ihrer Webserver-Umgebung Zugriff, um Protokolldateien auf Amazon S3 hochzuladen.

`AWSElasticBeanstalkWebTier`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkWebTier` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:08 UTC
- Bearbeitete Zeit: 9. September 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWebTier`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsAccess",
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Effect" : "Allow",
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticBeanstalkWorkerTier

Beschreibung: Geben Sie den Instances in Ihrer Arbeitsumgebung Zugriff, um Protokolldateien auf Amazon S3 hochzuladen, Amazon SQS zur Überwachung der Job-Warteschlange Ihrer Anwendung zu verwenden, Amazon DynamoDB für die Auswahl von Führungskräften zu verwenden und für Amazon, um Metriken für die Zustandsüberwachung CloudWatch zu veröffentlichen.

`AWSElasticBeanstalkWorkerTier`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSElasticBeanstalkWorkerTier` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Februar 2016, 23:12 UTC
- Bearbeitete Zeit: 9. September 2020, 19:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticBeanstalkWorkerTier`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MetricsAccess",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "XRayAccess",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "QueueAccess",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "BucketAccess",
      "Action" : [
        "s3:Get*",
        "s3:List*",
        "s3:PutObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::elasticbeanstalk-*",
        "arn:aws:s3:::elasticbeanstalk-*/*"
      ]
    },
    {
      "Sid" : "DynamoPeriodicTasks",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/*-stack-AWSEBWorkerCronLeaderRegistry*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsAccess",
```

```
      "Action" : [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/elasticbeanstalk*"
      ]
    },
    {
      "Sid" : "ElasticBeanstalkHealthAccess",
      "Action" : [
        "elasticbeanstalk:PutInstanceStatistics"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:elasticbeanstalk:*:*:application/*",
        "arn:aws:elasticbeanstalk:*:*:environment/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryAgentInstallationPolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation des AWS Replication Agent, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung externer Server verwendet wird AWS. Ordnen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen zu, deren Anmeldeinformationen Sie bei der Installation des AWS Replication Agent angeben.

`AWSElasticDisasterRecoveryAgentInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryAgentInstallationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:37 UTC
- Bearbeitete Zeit: 27. November 2023, 12:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryAgentInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateRecoveryInstanceForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSAgentInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy3",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateRecoveryInstanceForDrs"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy4",
      "Effect" : "Allow",
      "Action" : "drs:TagResource",
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
        }
      }
    },
    {
      "Sid" : "DRSAgentInstallationPolicy5",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryAgentPolicy

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des AWS Replication Agents, der zusammen mit AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wird AWS. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryAgentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryAgentPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:32 UTC
- Bearbeitete Zeit: 27. November 2023, 13:44 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryAgentPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSAgentPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/${aws:SourceIdentity}"
    },
    {
      "Sid" : "DRSAgentPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen Bereiche APIs von AWS Elastic Disaster Recovery (DRS) sowie Berechtigungen zum Lesen von KMS-Schlüsseln, License Manager, Resource Groups, Elastic Load Balancing, IAM und EC2 Informationen. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSElasticDisasterRecoveryConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:46 UTC
- Bearbeitete Zeit: 12. Januar 2025, 07:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
```

```
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
```

```
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
```

```
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConsoleFullAccess_v2

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf alle öffentlichen Dienste APIs von AWS Elastic Disaster Recovery (AWS DRS) sowie auf alle öffentlichen APIs AWS Dienste, die von der AWS DRS-Konsole verwendet werden. Fügen Sie diese Richtlinie Ihren Benutzern oder Rollen hinzu.

`AWSElasticDisasterRecoveryConsoleFullAccess_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryConsoleFullAccess_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2023, 13:35 UTC
- Bearbeitete Zeit: 2. Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryConsoleFullAccess_v2`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConsoleFullAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess2",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:DescribeKeyPairs",
```

```
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeHosts",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess4",
      "Effect" : "Allow",
      "Action" : "license-manager:ListLicenseConfigurations",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess5",
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess6",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess7",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess8",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess11",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess16",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSecurityGroup",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "ConsoleFullAccess17",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "ConsoleFullAccess20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:StartInstances",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess22",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess25",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
            "CreateNetworkInterface"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "ConsoleFullAccess27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess28",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess29",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess30",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess31",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-CreateImage:$DEFAULT",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess32",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess33",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConsoleFullAccess34",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess35",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "ConsoleFullAccess36",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess37",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess38",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ConsoleFullAccess39",
      "Effect" : "Allow",
      "Action" : "ec2:CreateFleet",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess40",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateFleet"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess41",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess42",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ConsoleFullAccess43",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ConsoleFullAccess44",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryConversionServerPolicy

Beschreibung: Diese Richtlinie ist der Instanzrolle des AWS Elastic Disaster Recovery Conversion-Servers zugeordnet. Diese Richtlinie ermöglicht es Elastic Disaster Recovery (DRS) - Konversionsservern, bei denen es sich um EC2 Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren. Eine IAM-Rolle mit dieser Richtlinie wird von DRS (als EC2 Instanzprofil) an die DRS-Konvertierungsserver angehängt, die bei Bedarf automatisch von DRS gestartet und beendet werden. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen. DRS-Konvertierungsserver werden von Elastic Disaster Recovery verwendet, wenn Benutzer Quellserver mithilfe der DRS-Konsole, CLI oder API wiederherstellen möchten.

`AWSElasticDisasterRecoveryConversionServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryConversionServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 13:42 UTC
- Bearbeitete Zeit: 27. November 2023, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryConversionServerPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSConversionServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSConversionServerPolicy2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryCrossAccountReplicationPolicy

Beschreibung: Diese Richtlinie ermöglicht es AWS Elastic Disaster Recovery (DRS), kontenübergreifende Replikation und kontenübergreifendes Failback zu unterstützen.

`AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryCrossAccountReplicationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Mai 2023, 07:16 UTC
- Bearbeitete Zeit: 17. Januar 2024, 13:19 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryCrossAccountReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CrossAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeInstances",
        "drs:DescribeSourceServers",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryEc2InstancePolicy

Beschreibung: Diese Richtlinie ermöglicht die Installation und Verwendung des AWS Replication Agents, der von AWS Elastic Disaster Recovery (DRS) zur Wiederherstellung von Quellservern verwendet wird, die auf EC2 (regionsübergreifend oder az-übergreifend) ausgeführt werden. Eine IAM-Rolle mit dieser Richtlinie sollte (als EC2 Instanzprofil) an die Instances angehängt werden. EC2

`AWSElasticDisasterRecoveryEc2InstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryEc2InstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 12:30 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryEc2InstancePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSEc2InstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:CreateSourceServerForDrs",
        "drs:CreateSourceNetwork"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-network/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceNetwork"
```

```
        }
      }
    },
    {
      "Sid" : "DRSEc2InstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSEc2InstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackInstallationPolicy

Beschreibung: Sie können die AWSElastic DisasterRecoveryFailbackInstallationPolicy Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie ermöglicht die Installation des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur verwendet wird. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu, deren Anmeldeinformationen Sie bei der Ausführung des Elastic Disaster Recovery Failback Client angeben.

`AWSElasticDisasterRecoveryFailbackInstallationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryFailbackInstallationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 11:02 UTC
- Bearbeitete Zeit: 27. November 2023, 13:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryFailbackInstallationPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackInstallationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientLogsForDrs",
        "drs:SendClientMetricsForDrs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeSourceServers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackInstallationPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource",
        "drs:IssueAgentCertificateForDrs",
        "drs:AssociateFailbackClientToRecoveryInstanceForDrs",
        "drs:GetSuggestedFailbackClientDeviceMappingForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateFailbackClientDeviceMappingForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryFailbackPolicy

Beschreibung: Diese Richtlinie ermöglicht die Verwendung des Elastic Disaster Recovery Failback Client, der für ein Failback von Wiederherstellungsinstanzen auf Ihre ursprüngliche Quellinfrastruktur verwendet wird. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSElasticDisasterRecoveryFailbackPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryFailbackPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:41 UTC
- Bearbeitete Zeit: 27. November 2023, 12:56 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryFailbackPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSFailbackPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeRecoveryInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSFailbackPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetFailbackCommandForDrs",
        "drs:UpdateFailbackClientLastSeenForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
```

```
        "drs:NotifyConsistencyAttainedForDrs",
        "drs:GetFailbackLaunchRequestedForDrs",
        "drs:IssueAgentCertificateForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/${aws:SourceIdentity}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryLaunchActionsPolicy

Beschreibung: Mit dieser Richtlinie können Sie Amazon SSM und weitere für Dienste erforderliche Berechtigungen verwenden, um Aktionen nach dem Start in AWS Elastic Disaster Recovery (AWS DRS) auszuführen. Fügen Sie diese Richtlinie Ihren IAM-Rollen oder -Benutzern hinzu.

`AWSElasticDisasterRecoveryLaunchActionsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryLaunchActionsPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. September 2023, 07:38 UTC
- Bearbeitete Zeit: 02. Juli 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryLaunchActionsPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LaunchActionsPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeParameters"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
```

```
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-*",
        "arn:aws:ssm:*::document/AWSCodeDeployAgent-*",
        "arn:aws:ssm:*::document/AWSConfigRemediation-*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSDisasterRecovery-*",
        "arn:aws:ssm:*::document/AWSDistroOTel-*",
        "arn:aws:ssm:*::document/AWSDocs-*",
        "arn:aws:ssm:*::document/AWSEC2-*",
        "arn:aws:ssm:*::document/AWSEC2Launch-*",
        "arn:aws:ssm:*::document/AWSFIS-*",
        "arn:aws:ssm:*::document/AWSFleetManager-*",
        "arn:aws:ssm:*::document/AWSIncidents-*",
        "arn:aws:ssm:*::document/AWSKinesisTap-*",
        "arn:aws:ssm:*::document/AWSMigration-*",
        "arn:aws:ssm:*::document/AWSNVMe-*",
        "arn:aws:ssm:*::document/AWSNitroEnclavesWindows-*",
        "arn:aws:ssm:*::document/AWSObservabilityExporter-*",
        "arn:aws:ssm:*::document/AWSPVDriver-*",
        "arn:aws:ssm:*::document/AWSQuickSetupType-*",
        "arn:aws:ssm:*::document/AWSQuickStarts-*",
        "arn:aws:ssm:*::document/AWSRefactorSpaces-*",
        "arn:aws:ssm:*::document/AWSResilienceHub-*",
        "arn:aws:ssm:*::document/AWSSAP-*",
        "arn:aws:ssm:*::document/AWSSAPTools-*",
```

```
        "arn:aws:ssm:*::document/AWSSQLServer-*",
        "arn:aws:ssm:*::document/AWSSSO-*",
        "arn:aws:ssm:*::document/AWSSupport-*",
        "arn:aws:ssm:*::document/AWSSystemsManagerSAP-*",
        "arn:aws:ssm:*::document/AmazonCloudWatch-*",
        "arn:aws:ssm:*::document/AmazonCloudWatchAgent-*",
        "arn:aws:ssm:*::document/AmazonECS-*",
        "arn:aws:ssm:*::document/AmazonEFSUtils-*",
        "arn:aws:ssm:*::document/AmazonEKS-*",
        "arn:aws:ssm:*::document/AmazonInspector-*",
        "arn:aws:ssm:*::document/AmazonInspector2-*",
        "arn:aws:ssm:*::document/AmazonInternal-*",
        "arn:aws:ssm:*::document/AwsEnaNetworkDriver-*",
        "arn:aws:ssm:*::document/AwsVssComponents-*",
        "arn:aws:ssm:*::automation-definition/AWS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSCodeDeployAgent-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConfigRemediation-*:*",
        "arn:aws:ssm:*::automation-definition/AWSConformancePacks-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDisasterRecovery-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDistroOTel-*:*",
        "arn:aws:ssm:*::automation-definition/AWSDocs-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2-*:*",
        "arn:aws:ssm:*::automation-definition/AWSEC2Launch-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFIS-*:*",
        "arn:aws:ssm:*::automation-definition/AWSFleetManager-*:*",
        "arn:aws:ssm:*::automation-definition/AWSIncidents-*:*",
        "arn:aws:ssm:*::automation-definition/AWSKinesisTap-*:*",
        "arn:aws:ssm:*::automation-definition/AWSMigration-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNVMe-*:*",
        "arn:aws:ssm:*::automation-definition/AWSNitroEnclavesWindows-*:*",
        "arn:aws:ssm:*::automation-definition/AWSObservabilityExporter-*:*",
        "arn:aws:ssm:*::automation-definition/AWSPVDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickSetupType-*:*",
        "arn:aws:ssm:*::automation-definition/AWSQuickStarts-*:*",
        "arn:aws:ssm:*::automation-definition/AWSRefactorSpaces-*:*",
        "arn:aws:ssm:*::automation-definition/AWSResilienceHub-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSAPTools-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSQLServer-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSSO-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSupport-*:*",
        "arn:aws:ssm:*::automation-definition/AWSSystemsManagerSAP-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatch-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonCloudWatchAgent-*:*",
```

```
        "arn:aws:ssm:*::automation-definition/AmazonECS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEFSUtils-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonEKS-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInspector2-*:*",
        "arn:aws:ssm:*::automation-definition/AmazonInternal-*:*",
        "arn:aws:ssm:*::automation-definition/AwsEnaNetworkDriver-*:*",
        "arn:aws:ssm:*::automation-definition/AwsVssComponents-*:*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSDRS" : "AllowLaunchingIntoThisInstance"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "drs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments",
        "ssm:ListCommandInvocations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchActionsPolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/*"
    },
    {
      "Sid" : "LaunchActionsPolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "LaunchActionsPolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/
ManagedByAWSElasticDisasterRecoveryService-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LaunchActionsPolicy11",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceWithLaunchActionsRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "drs.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryNetworkReplicationPolicy

Beschreibung: Diese Richtlinie ermöglicht es AWS Elastic Disaster Recovery (DRS), die Netzwerkreplikation zu unterstützen.

`AWSElasticDisasterRecoveryNetworkReplicationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryNetworkReplicationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. Juni 2023, 12:36 UTC
- Bearbeitete Zeit: 2. Januar 2024, 13:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryNetworkReplicationPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSNetworkReplicationPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeInstances",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReadOnlyAccess

Beschreibung: Sie können die AWSElastic DisasterRecoveryReadOnlyAccess Richtlinie an Ihre IAM-Identitäten anhängen. Diese Richtlinie gewährt allen öffentlichen Bereichen APIs von Elastic Disaster Recovery (DRS), die nur Lesezugriff haben, sowie einigen schreibgeschützten anderen AWS Diensten, die für die vollständige Nutzung APIs der DRS-Konsole mit Schreibschutz erforderlich sind. Fügen Sie diese Richtlinie Ihren IAM-Benutzern oder -Rollen hinzu.

`AWSElasticDisasterRecoveryReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2021, 10:50 UTC
- Bearbeitete Zeit: 29. Juli 2024, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElasticDisasterRecoveryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReadOnlyAccess1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeRecoveryInstances",
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "drs:ListLaunchActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:GetInstanceTypesFromInstanceRequirements"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess4",
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "DRSReadOnlyAccess5",
      "Effect" : "Allow",
      "Action" : "ssm:ListCommandInvocations",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReadOnlyAccess6",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameter",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSElasticDisasterRecovery-*"
    },
    {
      "Sid" : "DRSReadOnlyAccess7",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-CreateImage",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateNetworkConnectivity",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyMountedVolumes",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateHttpResponse",
        "arn:aws:ssm:*:*:document/AWSMigration-ValidateDiskSpace",
        "arn:aws:ssm:*:*:document/AWSMigration-VerifyProcessIsRunning",
        "arn:aws:ssm:*:*:document/AWSMigration-LinuxTimeSyncSetting",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure"
      ]
    },
    {
      "Sid" : "DRSReadOnlyAccess8",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "arn:aws:ssm:*:*:automation-execution/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryRecoveryInstancePolicy

Beschreibung: Diese Richtlinie ist an die Instanzrolle der Wiederherstellungsinstanz von Elastic Disaster Recovery angehängt. Diese Richtlinie ermöglicht es der Elastic Disaster Recovery (DRS) Recovery Instance, bei denen es sich um EC2 Instances handelt, die von Elastic Disaster Recovery gestartet wurden, mit dem DRS-Service zu kommunizieren und ein Failback auf ihre ursprüngliche Quellinfrastruktur durchzuführen. Eine IAM-Rolle mit dieser Richtlinie wird (als EC2 Instanzprofil) von Elastic Disaster Recovery den DRS-Wiederherstellungsinstanzen zugewiesen. Wir empfehlen nicht, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryRecoveryInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryRecoveryInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 10:20 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 13:11 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryRecoveryInstancePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSRecoveryInstancePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs",
        "drs:UpdateReplicationCertificateForDrs",
        "drs:NotifyReplicationServerAuthenticationForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*",
      "Condition" : {
        "StringEquals" : {
          "drs:EC2InstanceARN" : "${ec2:SourceInstanceARN}"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeRecoveryInstances"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy4",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentInstallationAssetsForDrs",
        "drs:SendClientLogsForDrs",
        "drs:CreateSourceServerForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy5",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*",
      "Condition" : {
        "StringEquals" : {
          "drs:CreateAction" : "CreateSourceServerForDrs"
        }
      }
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendAgentMetricsForDrs",
        "drs:SendAgentLogsForDrs",
        "drs:UpdateAgentSourcePropertiesForDrs",
        "drs:UpdateAgentReplicationInfoForDrs",
        "drs:UpdateAgentConversionInfoForDrs",
        "drs:GetAgentCommandForDrs",
```

```
        "drs:GetAgentConfirmedResumeInfoForDrs",
        "drs:GetAgentRuntimeConfigurationForDrs",
        "drs:UpdateAgentBacklogForDrs",
        "drs:GetAgentReplicationInfoForDrs"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSRecoveryInstancePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/DRSCrossAccountAgentAuthorizedRole_*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SourceInstanceARN" : "${ec2:SourceInstanceARN}"
        },
        "ForAnyValue:StringEquals" : {
          "sts:TransitiveTagKeys" : "SourceInstanceARN"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryReplicationServerPolicy

Beschreibung: Diese Richtlinie ist der Instance-Rolle des Elastic Disaster Recovery Replication-Servers zugeordnet. Diese Richtlinie ermöglicht es den Elastic Disaster Recovery (DRS) Replication Servern, bei denen es sich um EC2 Instances handelt, die von Elastic Disaster Recovery gestartet werden, mit dem DRS-Service zu kommunizieren und EBS-Snapshots in Ihrem zu erstellen. AWS-Konto Eine IAM-Rolle mit dieser Richtlinie wird (als EC2 Instanzprofil) von Elastic Disaster Recovery den DRS-Replikationsservern zugewiesen, die bei Bedarf automatisch von DRS gestartet und beendet werden. DRS-Replikationsserver werden verwendet, um die Datenreplikation von Ihren externen Servern auf AWS die Daten als Teil des von DRS verwalteten Wiederherstellungsprozesses zu erleichtern. Es wird nicht empfohlen, diese Richtlinie Ihren IAM-Benutzern oder -Rollen zuzuordnen.

`AWSElasticDisasterRecoveryReplicationServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryReplicationServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. November 2021, 13:34 UTC
- Bearbeitete Zeit: 27. November 2023, 13:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryReplicationServerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSReplicationServerPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:SendClientMetricsForDrs",
        "drs:SendClientLogsForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetChannelCommandsForDrs",
        "drs:SendChannelCommandResultForDrs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:GetAgentSnapshotCreditsForDrs",
        "drs:DescribeReplicationServerAssociationsForDrs",
        "drs:DescribeSnapshotRequestsForDrs",
        "drs:BatchDeleteSnapshotRequestForDrs",
        "drs:NotifyAgentAuthenticationForDrs",
        "drs:BatchCreateVolumeSnapshotGroupForDrs",
        "drs:UpdateAgentReplicationProcessStateForDrs",
        "drs:NotifyAgentReplicationProgressForDrs",
        "drs:NotifyAgentConnectedForDrs",
        "drs:NotifyAgentDisconnectedForDrs",
        "drs:NotifyVolumeEventForDrs",
        "drs:SendVolumeStatsForDrs"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "DRSReplicationServerPolicy4",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSReplicationServerPolicy5",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSReplicationServerPolicy7",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSnapshot"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht Elastic Disaster Recovery, AWS Ressourcen in Ihrem Namen zu verwalten.

`AWSElasticDisasterRecoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 10:56 UTC
- Bearbeitete Zeit: 5. Januar 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticDisasterRecoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSServiceRolePolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy2",
      "Effect" : "Allow",
      "Action" : [
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:recovery-instance/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy3",
      "Effect" : "Allow",
      "Action" : [
        "drs:CreateRecoveryInstanceForDrs",
        "drs:TagResource"
      ],
      "Resource" : "arn:aws:drs:*:*:source-server/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy4",
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy5",
```

```
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy6",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeAttribute",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeRouteTables",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RegisterImage"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeregisterImage"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy10",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "DRSServiceRolePolicy11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy13",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy14",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy15",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy16",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
```

```
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy18",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy19",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy20",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume",
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DRSServiceRolePolicy21",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DetachVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Sid" : "DRSServiceRolePolicy23",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy24",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy25",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryReplicationServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryConversionServerRole",
        "arn:aws:iam::*:role/service-role/
AWSElasticDisasterRecoveryRecoveryInstanceRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy26",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateLaunchTemplate",
            "CreateSecurityGroup",
            "CreateVolume",
            "CreateSnapshot",
            "RunInstances",
```

```
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy27",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy28",
      "Effect" : "Allow",
      "Action" : "cloudwatch:GetMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "DRSServiceRolePolicy29",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy30",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
```

```
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy31",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DRSServiceRolePolicy32",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSServiceRolePolicy33",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy

Beschreibung: Diese Richtlinie ermöglicht den schreibgeschützten Zugriff auf AWS Elastic Disaster Recovery (DRS) -Ressourcen wie Quellserver und Jobs. Sie ermöglicht auch die Erstellung eines konvertierten Snapshots und die gemeinsame Nutzung dieses EBS-Snapshots mit einem bestimmten Konto.

`AWSElasticDisasterRecoveryStagingAccountPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryStagingAccountPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Mai 2022, 09:49 UTC
- Bearbeitete Zeit: 27. November 2023, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicy1",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicy2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticDisasterRecoveryStagingAccountPolicy_v2

Beschreibung: Diese Richtlinie wird von AWS Elastic Disaster Recovery (DRS) verwendet, um Quellserver in einem separaten Zielkonto wiederherzustellen und ein Failback zu ermöglichen. Es wird nicht empfohlen, diese Richtlinie an Ihre IAM-Benutzer oder -Rollen anzuhängen.

`AWSElasticDisasterRecoveryStagingAccountPolicy_v2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElasticDisasterRecoveryStagingAccountPolicy_v2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Januar 2023, 12:11 UTC
- Bearbeitete Zeit: 27. November 2023, 13:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSElasticDisasterRecoveryStagingAccountPolicy_v2`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DRSStagingAccountPolicyv21",
      "Effect" : "Allow",
      "Action" : [
        "drs:DescribeSourceServers",
        "drs:DescribeRecoverySnapshots",
        "drs:CreateConvertedSnapshotForDrs",
        "drs:GetReplicationConfiguration",
        "drs:DescribeJobs",
        "drs:DescribeJobLogItems"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DRSStagingAccountPolicyv22",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Add/userId" : "${aws:SourceIdentity}"
        },
        "Null" : {
          "aws:ResourceTag/AWSElasticDisasterRecoveryManaged" : "false"
        }
      }
    },
    {
      "Sid" : "DRSStagingAccountPolicyv23",
      "Effect" : "Allow",
      "Action" : "drs:IssueAgentCertificateForDrs",
      "Resource" : [
        "arn:aws:drs:*:*:source-server/*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticLoadBalancingClassicServiceRolePolicy

Beschreibung: Service Linked Role Policy für AWS Elastic Load Balancing Control Plane — Classic

`AWSElasticLoadBalancingClassicServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. September 2017, 22:36 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingClassicServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElasticLoadBalancingServiceRolePolicy

Beschreibung: Service Linked Role Policy für die AWS Elastic Load Balancing Control Plane

`AWSElasticLoadBalancingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. September 2017, 22:19 Uhr UTC
- Bearbeitete Zeit: 17. November 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSElasticLoadBalancingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeCoipPools",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeVpcClassicLink",
        "ec2:CreateSecurityGroup",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssignIpv6Addresses",
        "ec2:ReleaseAddress",
        "ec2:UnassignIpv6Addresses",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeAvailabilityZones",
        "ec2:AllocateIpamPoolCidr",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
```

```
        "outposts:GetOutpostInstanceTypes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConnectFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare MediaConnect Ressourcen.

`AWSElementalMediaConnectFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaConnectFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Februar 2025, 20:07 UTC
- Bearbeitete Zeit: 12. Februar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConnectReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS MediaConnect Elementar-Ressourcen.

`AWSElementalMediaConnectReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaConnectReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Februar 2025, 20:07 UTC
- Bearbeitete Zeit: 12. Februar 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConnectReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:ListBridges",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListGatewayInstances",
        "mediaconnect:ListGateways",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:DescribeBridge",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeFlowSourceMetadata",
        "mediaconnect:DescribeFlowSourceThumbnail",
        "mediaconnect:DescribeGateway",
        "mediaconnect:DescribeGatewayInstance",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListTagsForResource"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConvertFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Elemental MediaConvert über das SDK AWS-Managementkonsole und.

`AWSElementalMediaConvertFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaConvertFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2018, 19:25 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "mediaconvert.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaConvertReadOnly

Beschreibung: Bietet MediaConvert über das SDK AWS-Managementkonsole und den Lesezugriff auf AWS Elemental.

`AWSElementalMediaConvertReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaConvertReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juni 2018, 19:25 UTC
- Bearbeitete Zeit: 10. Juni 2019, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaConvertReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "mediaconvert:DescribeEndpoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaLiveFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaLive

`AWSElementalMediaLiveFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaLiveFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juli 2020, 17:07 UTC
- Bearbeitete Zeit: 8. Juli 2020, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "medialive:*",
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaLiveReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaLive

`AWSElementalMediaLiveReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaLiveReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Juli 2020, 16:38 UTC
- Bearbeitete Zeit: 22. Juli 2024, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaLiveReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSElementalMediaLiveReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "medialive:Get*",
        "medialive:List*",
        "medialive:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaPackage

`AWSElementalMediaPackageFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaPackageFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. Dezember 2017, 23:39 Uhr UTC
- Zeit bearbeitet: 29. Dezember 2017, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
```

```
    "Action" : "mediapackage:*",
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaPackage

`AWSElementalMediaPackageReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaPackageReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Dezember 2017, 00:04 Uhr UTC
- Zeit bearbeitet: 30. Dezember 2017, 00:04 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackage:List*",
      "mediapackage:Describe*"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageV2FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Elemental MediaPackage V2-Ressourcen.

`AWSElementalMediaPackageV2FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaPackageV2FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 25. Juli 2023, 20:29 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2FullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediapackagev2:*",
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaPackageV2ReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elemental V2-Ressourcen MediaPackage.

`AWSElementalMediaPackageV2ReadOnly`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaPackageV2ReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 20:31 UTC
- Bearbeitete Zeit: 25. Juli 2023, 20:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaPackageV2ReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediapackagev2:List*",
      "mediapackagev2:Get*"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaStoreFullAccess

Beschreibung: Bietet vollen Lese- und Schreibzugriff für alle MediaStore APIs

`AWSElementalMediaStoreFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaStoreFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. März 2018, 23:15 Uhr UTC
- Bearbeitete Zeit: 5. März 2018, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Action" : [
        "mediastore:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaStoreReadOnly

Beschreibung: Bietet Nur-Lese-Berechtigungen für MediaStore APIs

`AWSElementalMediaStoreReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaStoreReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. März 2018, 19:48 UTC

- Bearbeitete Zeit: 8. März 2018, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaStoreReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mediastore:Get*",
        "mediastore:List*",
        "mediastore:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:SecureTransport" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaTailorFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS elementare Ressourcen MediaTailor

`AWSElementalMediaTailorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaTailorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. November 2021, 00:04 Uhr UTC
- Bearbeitete Zeit: 23. November 2021, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : "mediatailor:*",
    "Resource" : "*"
```

```
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSElementalMediaTailorReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Elementar-Ressourcen MediaTailor

`AWSElementalMediaTailorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSElementalMediaTailorReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. November 2021, 00:05 Uhr UTC
- Bearbeitete Zeit: 23. November 2021, 00:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSElementalMediaTailorReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "mediatailor:List*",
      "mediatailor:Describe*",
      "mediatailor:Get*"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEnhancedClassicNetworkingMangementPolicy

Beschreibung: Richtlinie zur Aktivierung der erweiterten klassischen Netzwerkverwaltungsfunktion.

`AWSEnhancedClassicNetworkingMangementPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. September 2017, 17:29 Uhr UTC

- Zeit bearbeitet: 20. September 2017, 17:29 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSEnhancedClassicNetworkingMangementPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEntityResolutionConsoleFullAccess

Beschreibung: Bietet vollen Konsolenzugriff auf AWS Entity Resolution und verwandte Dienste.

`AWSEntityResolutionConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSEntityResolutionConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. August 2023, 17:54 UTC
- Bearbeitete Zeit: 15. Dezember 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:GetSchema",
        "glue:SearchTables",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersion",
        "glue:GetTableVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3BucketsConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3SourcesConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions",
        "s3:GetBucketVersioning"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TaggingConsoleDisplay",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMSConsoleDisplay",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListRolesToPickRoleForPassing",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEntityResolutionService",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*entityresolution*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "entityresolution.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ManageEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/entity-resolution-automatic*"
      ]
    },
    {
      "Sid" : "ADXReadAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "dataexchange:GetDataSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "connect:ListInstances",
        "profile:ListDomains",
        "profile:GetDomain",
        "profile:ListIntegrations",
        "profile:ListAccountIntegrations",
        "profile:ListProfileObjectTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CustomerProfilesIntegrationWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "profile:PutProfileObjectType"
      ],
      "Resource" : [
        "arn:aws:profile:*:*:domains/*/object-types/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSEntityResolutionConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Entity Resolution über die. AWS-Managementkonsole

`AWSEntityResolutionConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSEntityResolutionConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. August 2023, 18:18 UTC
- Bearbeitete Zeit: 17. August 2023, 18:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSEntityResolutionConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EntityResolutionRead",
      "Effect" : "Allow",
      "Action" : [
        "entityresolution:Get*",
        "entityresolution:List*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEC2Access

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator-Dienst die Berechtigung für die Ausführung von FIS-Aktionen EC2 und anderen erforderlichen Diensten.

`AWSFaultInjectionSimulatorEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorEC2Access` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:39 UTC
- Bearbeitete Zeit: 11. November 2025, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEC2Access`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowEc2Actions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:SendSpotInstanceInterruptions",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "AllowEc2InstancesWithEncryptedEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
      }
    },
    {
      "Sid" : "AllowSSMSendOnEc2",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Sid" : "AllowSSMStopOnEc2",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:ListCommands"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorECSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in ECS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorECSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorECSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:37 UTC
- Bearbeitete Zeit: 11. November 2025, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorECSAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Clusters",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
```

```
        "ecs:ListContainerInstances"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "Tasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTasks",
        "ecs:StopTask"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task/*/*"
      ]
    },
    {
      "Sid" : "ContainerInstances",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:container-instance/*/*"
      ]
    },
    {
      "Sid" : "ListTasks",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMSend",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
```

```
    {
      "Sid" : "SSMList",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeContainerInstances",
      "Effect" : "Allow",
      "Action" : "ecs:DescribeContainerInstances",
      "Resource" : "arn:aws:ecs:*:*:container-instance/*/*"
    },
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorEKSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in EKS und anderen erforderlichen Diensten die Berechtigung, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorEKSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorEKSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:34 UTC
- Bearbeitete Zeit: 11. März 2025, 14:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorEKSAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "DescribeInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstances",
      "Resource" : "*"
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Sid" : "DescribeSubnets",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSubnets",
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeCluster",
      "Effect" : "Allow",
      "Action" : "eks:DescribeCluster",
      "Resource" : "arn:aws:eks:*:*:cluster/*"
    },
    {
      "Sid" : "DescribeNodeGroup",
      "Effect" : "Allow",
      "Action" : "eks:DescribeNodegroup",
      "Resource" : "arn:aws:eks:*:*:nodegroup/*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorNetworkAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service die Erlaubnis, EC2 Netzwerke und andere erforderliche Dienste auszuführen, um FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorNetworkAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorNetworkAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:32 UTC
- Bearbeitete Zeit: 11. März 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorNetworkAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateTagsOnNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkAcl",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkAcl",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-acl/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
```

```
      }
    },
    {
      "Sid" : "CreateNetworkAclOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkAcl",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "VpcActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReplaceNetworkAclAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceNetworkAclAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-acl/*"
      ]
    },
    {
      "Sid" : "GetManagedPrefixListEntries",
      "Effect" : "Allow",
      "Action" : "ec2:GetManagedPrefixListEntries",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*"
    },
    {
      "Sid" : "CreateRouteTable",
      "Effect" : "Allow",
```

```
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableOnVpc",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRouteTable",
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "CreateTagsOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsOnPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "ec2:CreateAction" : "CreateManagedPrefixList",
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : "ec2:CreateRoute",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaceOnSubnet",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteNetworkInterface",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "CreateManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:CreateManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteManagedPrefixList",
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyManagedPrefixList",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyManagedPrefixList",
```

```
      "Resource" : "arn:aws:ec2:*:*:prefix-list/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ReplaceRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : "ec2:ReplaceRouteTableAssociation",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:AssociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "DisassociateRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "DisassociateRouteTableOnSubnet",
      "Effect" : "Allow",
      "Action" : "ec2:DisassociateRouteTable",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
```

```
      ]
    },
    {
      "Sid" : "ModifyVpcEndpointOnRouteTable",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/managedByFIS" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoint",
      "Effect" : "Allow",
      "Action" : "ec2:ModifyVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ]
    },
    {
      "Sid" : "TransitGatewayRouteTableAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:AssociateTransitGatewayRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*",
        "arn:aws:ec2:*:*:transit-gateway-attachment/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorRDSAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in RDS und anderen erforderlichen Diensten die Erlaubnis, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorRDSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorRDSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 20:30 Uhr UTC
- Bearbeitete Zeit: 18. März 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorRDSAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AllowFailover",
      "Effect" : "Allow",
      "Action" : [
        "rds:FailoverDBCluster"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:cluster:*"
      ]
    },
    {
      "Sid" : "AllowReboot",
      "Effect" : "Allow",
      "Action" : [
        "rds:RebootDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:db:*"
      ]
    },
    {
      "Sid" : "DescribeResources",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TargetResolutionByTags",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFaultInjectionSimulatorSSMAccess

Beschreibung: Diese Richtlinie gewährt dem Fault Injection Simulator Service in SSM und anderen erforderlichen Diensten die Berechtigung, FIS-Aktionen auszuführen.

`AWSFaultInjectionSimulatorSSMAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFaultInjectionSimulatorSSMAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. Oktober 2022, 15:33 UTC
- Bearbeitete Zeit: 25. Juni 2025, 14:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSFaultInjectionSimulatorSSMAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:ListCommands",
        "ssm:CancelCommand"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFinSpaceServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung des Zugriffs auf AWS-Service und von Amazon verwendete oder verwaltete Ressourcen FinSpace

`AWSFinSpaceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Mai 2023, 16:42 UTC
- Bearbeitete Zeit: 1. Dezember 2023, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSFinSpaceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSFinSpaceServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/FinSpace",
            "AWS/Usage"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMAdminFullAccess

Beschreibung: Voller Zugriff für AWS FM Administrator

`AWSFMAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFMAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Mai 2018, 18:06 UTC
- Zeit bearbeitet: 20. Oktober 2022, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
```

```
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "fms.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
```

```
        "organizations:ListDelegatedAdministrators",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMAdminReadOnlyAccess

Beschreibung: Nur-Lese-Zugriff für AWS FM Administrator, der die Überwachung von AWS FM-Vorgängen ermöglicht

`AWSFMAdminReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFMAdminReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Mai 2018, 20:07 UTC

- Bearbeitete Zeit: 31. Oktober 2022, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMAdminReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fms:Get*",
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
```

```
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "fms.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSFMMemberReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF-Aktionen für AWS Firewall Manager Manager-Mitgliedskonten

`AWSFMMemberReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSFMMemberReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2018, 21:05 UTC
- Bearbeitete Zeit: 9. Mai 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSFMMemberReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "fms:GetAdminAccount",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "organizations:DescribeOrganization"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSForWordPressPluginPolicy

Beschreibung: Verwaltete Richtlinie für das AWS For Wordpress Plugin

`AWSForWordPressPluginPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSForWordPressPluginPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Oktober 2019, 00:27 UTC
- Bearbeitete Zeit: 20. Januar 2020, 23:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSForWordPressPluginPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Permissions1",
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech",
        "polly:DescribeVoices",
        "translate:TranslateText"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Permissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:CreateBucket",
        "s3:PutObjectAcl"
      ],
      "Resource" : [
        "arn:aws:s3:::audio_for_wordpress*",
        "arn:aws:s3:::audio-for-wordpress*"
      ]
    },
    {
      "Sid" : "Permissions3",
      "Effect" : "Allow",
      "Action" : [
        "acm:AddTagsToCertificate",
        "acm:DescribeCertificate",
        "acm:RequestCertificate",
        "cloudformation:CreateStack",
```

```
        "cloudfront:ListDistributions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestedRegion" : "us-east-1"
        }
      }
    },
    {
      "Sid" : "Permissions4",
      "Effect" : "Allow",
      "Action" : [
        "acm:DeleteCertificate",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:UpdateStack",
        "cloudfront:CreateDistribution",
        "cloudfront:CreateInvalidation",
        "cloudfront:DeleteDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetInvalidation",
        "cloudfront:TagResource",
        "cloudfront:UpdateDistribution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/createdBy" : "AWSForWordPressPlugin"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGitSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Code Connections ermöglicht, Inhalte aus Ihrem Git-Repository zu synchronisieren

`AWSGitSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2023, 17:05 UTC
- Bearbeitete Zeit: 26. April 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGitSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlobalAcceleratorSLRPolicy

Beschreibung: Richtlinie, die AWS Global Accelerator Berechtigungen zur Verwaltung von EC2 Elastic Network Interfaces und Security Groups gewährt.

`AWSGlobalAcceleratorSLRPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. April 2019, 19:39 UTC
- Bearbeitete Zeit: 29. Oktober 2024, 18:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSGlobalAcceleratorSLRPolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Action1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action2",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSServiceName" : "GlobalAccelerator"
        }
      }
    },
    {
      "Sid" : "EC2Action3",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:GetSecurityGroupsForVpc"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ElbAction1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Action4",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Glue über die AWS-Managementkonsole

`AWSGlueConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 13:37 UTC
- Bearbeitete Zeit: 14. Juli 2023, 14:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "BaseAppPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBSubnetGroups",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:DescribeRecipe"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueConsoleSageMakerNotebookFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Glue über die AWS-Managementkonsole und Zugriff auf Sagemaker-Notebook-Instanzen.

`AWSGlueConsoleSageMakerNotebookFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueConsoleSageMakerNotebookFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Oktober 2018, 17:52 Uhr UTC
- Bearbeitete Zeit: 15. Juli 2021, 15:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueConsoleSageMakerNotebookFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "iam:ListRoles",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "rds:DescribeDBInstances",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "dynamodb:ListTables",
        "kms:ListAliases",
        "kms:DescribeKey",
        "sagemaker:ListNotebookInstances",
```

```
        "cloudformation:ListStacks",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListDashboards"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*aws-glue-*/*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/aws-glue*/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedNotebookInstanceUrl",
        "sagemaker:CreateNotebookInstance",
        "sagemaker:DeleteNotebookInstance",
        "sagemaker:DescribeNotebookInstance",
        "sagemaker:StartNotebookInstance",
        "sagemaker:StopNotebookInstance",
        "sagemaker:UpdateNotebookInstance",
        "sagemaker:ListTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance/aws-glue-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeNotebookInstanceLifecycleConfig",
        "sagemaker:CreateNotebookInstanceLifecycleConfig",
        "sagemaker:DeleteNotebookInstanceLifecycleConfig",
        "sagemaker:ListNotebookInstanceLifecycleConfigs"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:notebook-instance-lifecycle-config/aws-glue-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/aws-glue-*/*"
        },
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ZeppelinInstance"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/AWSGlueServiceSageMakerNotebookRole*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AWSGlueServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueDataBrewFullAccessPolicy

Beschreibung: Bietet vollen Zugriff auf AWS Glue DataBrew über die AWS-Managementkonsole. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, KMS, Glue).

`AwsGlueDataBrewFullAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AwsGlueDataBrewFullAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. November 2020, 16:51 UTC
- Zeit bearbeitet: 4. Februar 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueDataBrewFullAccessPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "databrew:CreateDataset",
        "databrew:DescribeDataset",
        "databrew:ListDatasets",
        "databrew:UpdateDataset",
        "databrew:DeleteDataset",
        "databrew:CreateProject",
        "databrew:DescribeProject",
        "databrew:ListProjects",
        "databrew:StartProjectSession",
        "databrew:SendProjectSessionAction",
        "databrew:UpdateProject",
        "databrew:DeleteProject",
        "databrew:CreateRecipe",
        "databrew:DescribeRecipe",
        "databrew:ListRecipes",
        "databrew:ListRecipeVersions",
        "databrew:PublishRecipe",
        "databrew:UpdateRecipe",
        "databrew:BatchDeleteRecipeVersion",
        "databrew:DeleteRecipeVersion",
        "databrew:CreateRecipeJob",
        "databrew:CreateProfileJob",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:StartJobRun",
        "databrew:StopJobRun",
        "databrew:UpdateProfileJob",
        "databrew:UpdateRecipeJob",
```

```
        "databrew:DeleteJob",
        "databrew:CreateSchedule",
        "databrew:DescribeSchedule",
        "databrew:ListSchedules",
        "databrew:UpdateSchedule",
        "databrew:DeleteSchedule",
        "databrew:CreateRuleset",
        "databrew:DeleteRuleset",
        "databrew:DescribeRuleset",
        "databrew:ListRulesets",
        "databrew:UpdateRuleset",
        "databrew:ListTagsForResource",
        "databrew:TagResource",
        "databrew:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetDataCatalogEncryptionSettings",
        "dataexchange:ListDataSets",
        "dataexchange:ListDataSetRevisions",
        "dataexchange:ListRevisionAssets",
        "dataexchange:CreateJob",
        "dataexchange:StartJob",
        "dataexchange:GetJob",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
```

```
        "redshift:DescribeClusters",
        "redshift:DescribeClusterSubnetGroups",
        "redshift-data:DescribeStatement",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "s3:ListAllMyBuckets",
        "s3:GetBucketCORS",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "secretsmanager:ListSecrets",
        "secretsmanager:DescribeSecret",
        "sts:GetCallerIdentity",
        "cloudtrail:LookupEvents",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/AwsGlueDataBrew-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreateTable"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*/awsgluedatabrew*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AwsGlueDataBrew-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateRandom"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "databrew!default"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "databrew.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "databrew.amazonaws.com"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueDataBrewServiceRole

Beschreibung: Diese Richtlinie gewährt Glue die Erlaubnis, Aktionen für den Glue-Datenkatalog des Benutzers auszuführen. Diese Richtlinie gewährt auch die Erlaubnis für ec2-Aktionen, damit Glue ENI erstellen kann, um eine Verbindung zu Ressourcen in der VPC herzustellen, Glue auch den Zugriff auf registrierte Daten in Lakeformation und die Erlaubnis, auf die Cloudwatch des Benutzers zuzugreifen

`AWSGlueDataBrewServiceRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSGlueDataBrewServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 4. Dezember 2020, 21:26 Uhr UTC
- Bearbeitete Zeit: 20. März 2024, 23:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueDataBrewServiceRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetConnection"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePIIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:BatchGetCustomEntityTypes",
        "glue:GetCustomEntityType"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3PublicDatasetAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::databrew-public-datasets-*"
      ]
    },
    {
      "Sid" : "EC2NetworkingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DeleteGlueNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws-glue-service-resource" : "*"
        }
      },
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2GlueTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "GlueDatabrewLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws-glue-databrew/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:databrew!default-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueSchemaRegistryFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueSchemaRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 00:19 UTC
- Zeit bearbeitet: 20. November 2020, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateRegistry",
        "glue:UpdateRegistry",
        "glue:DeleteRegistry",
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:CreateSchema",
        "glue:UpdateSchema",
        "glue:DeleteSchema",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:RegisterSchemaVersion",
        "glue:DeleteSchemaVersions",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:ListSchemaVersions",
        "glue:CheckSchemaVersionValidity",
        "glue:PutSchemaVersionMetadata",
        "glue:RemoveSchemaVersionMetadata",
        "glue:QuerySchemaVersionMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSGlueSchemaRegistryTagsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTags",
        "glue:TagResource",
        "glue:UnTagResource"
      ],
      "Resource" : [
```

```
        "arn:aws:glue:*:*:schema/*",
        "arn:aws:glue:*:*:registry/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueSchemaRegistryReadonlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Glue Schema Registry Service

`AWSGlueSchemaRegistryReadonlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueSchemaRegistryReadonlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2020, 00:20 UTC
- Zeit bearbeitet: 20. November 2020, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGlueSchemaRegistryReadonlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGlueSchemaRegistryReadonlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetRegistry",
        "glue:ListRegistries",
        "glue:GetSchema",
        "glue:ListSchemas",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:ListSchemaVersions",
        "glue:GetSchemaVersionsDiff",
        "glue:CheckSchemaVersionValidity",
        "glue:QuerySchemaVersionMetadata",
        "glue:GetTags"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueServiceNotebookRole

Beschreibung: Richtlinie für die AWS Glue-Servicerolle, die es dem Kunden ermöglicht, den Notebook-Server zu verwalten

`AWSGlueServiceNotebookRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueServiceNotebookRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 UTC
- Bearbeitete Zeit: 9. Oktober 2023, 15:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceNotebookRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:CreatePartition",
        "glue:CreateTable",
        "glue:DeleteDatabase",
        "glue:DeletePartition",
```

```
        "glue:DeleteTable",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:CreateConnection",
        "glue:CreateJob",
        "glue:DeleteConnection",
        "glue:DeleteJob",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobs",
        "glue:UpdateJob",
        "glue:BatchDeleteConnection",
        "glue:UpdateConnection",
        "glue:GetUserDefinedFunction",
        "glue:UpdateUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:DeleteUserDefinedFunction",
        "glue:CreateUserDefinedFunction",
        "glue:BatchGetPartition",
        "glue:BatchDeletePartition",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteTable",
        "glue:UpdateDevEndpoint",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGlueServiceRole

Beschreibung: Richtlinie für die AWS Glue-Dienstrolle, die den Zugriff auf verwandte Dienste wie EC2 S3 und Cloudwatch Logs ermöglicht

`AWSGlueServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGlueServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:37 Uhr UTC
- Bearbeitete Zeit: 11. September 2023, 16:39 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:*",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeRouteTables",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "iam:ListRolePolicies",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
```

```
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*",
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
```

```
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookPolicy

Beschreibung: Stellt Berechtigungen bereit, die es Benutzern ermöglichen, nur die Notizbuchsitzungen zu erstellen und zu verwenden, die dem Benutzer zugeordnet sind. Diese Richtlinie beinhaltet auch Berechtigungen, die es Benutzern ausdrücklich ermöglichen, eine eingeschränkte Glue-Sitzungsrolle zu übergeben.

`AwsGlueSessionUserRestrictedNotebookPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AwsGlueSessionUserRestrictedNotebookPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. April 2022, 15:24 UTC
- Bearbeitete Zeit: 15. August 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedNotebookPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NotebokAllowActions0",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions1",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "NotebookAllowActions2",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Sid" : "NotebookAllowActions3",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "NotebookDenyActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "NotebookPassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/
AwsGlueSessionServiceRoleUserRestrictedForNotebook*",
        "arn:aws:iam::*:role/AwsGlueSessionUserRestrictedNotebookServiceRole*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedNotebookServiceRole

Beschreibung: Bietet vollen Zugriff auf alle AWS Glue-Ressourcen mit Ausnahme von Sitzungen. Ermöglicht Benutzern, nur die Notebook-Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie umfasst auch andere Berechtigungen, die Glue benötigt, um AWS Glue-Ressourcen in anderen AWS Diensten zu verwalten.

`AwsGlueSessionUserRestrictedNotebookServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AwsGlueSessionUserRestrictedNotebookServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. April 2022, 15:27 UTC
- Bearbeitete Zeit: 15. August 2024, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedNotebookServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}",
          "aws:RequestTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:PrincipalTag/owner}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedPolicy

Beschreibung: Stellt Berechtigungen bereit, die es Benutzern ermöglichen, nur die interaktiven Sitzungen zu erstellen und zu verwenden, die dem Benutzer zugeordnet sind. Diese Richtlinie beinhaltet auch Berechtigungen, die es Benutzern ausdrücklich ermöglichen, eine eingeschränkte Glue-Sitzungsrolle zu übergeben.

`AwsGlueSessionUserRestrictedPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AwsGlueSessionUserRestrictedPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. April 2022, 21:31 UTC
- Bearbeitete Zeit: 5. August 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AwsGlueSessionUserRestrictedPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
```

```
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AwsGlueSessionServiceRoleUserRestricted*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AwsGlueSessionUserRestrictedServiceRole

Beschreibung: Bietet vollen Zugriff auf alle AWS Glue-Ressourcen mit Ausnahme von Sitzungen. Ermöglicht Benutzern, nur die interaktiven Sitzungen zu erstellen und zu verwenden, die mit dem Benutzer verknüpft sind. Diese Richtlinie umfasst auch andere Berechtigungen, die Glue benötigt, um AWS Glue-Ressourcen in anderen AWS Diensten zu verwalten

`AwsGlueSessionUserRestrictedServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AwsGlueSessionUserRestrictedServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. April 2022, 21:30 UTC
- Bearbeitete Zeit: 5. August 2024, 23:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AwsGlueSessionUserRestrictedServiceRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowGlueActions",
      "Effect" : "Allow",
```

```
      "Action" : "glue:*",
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:tableVersion/*",
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:userDefinedFunction/*",
        "arn:aws:glue:*:*:devEndpoint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:trigger/*",
        "arn:aws:glue:*:*:crawler/*",
        "arn:aws:glue:*:*:workflow/*",
        "arn:aws:glue:*:*:mlTransform/*",
        "arn:aws:glue:*:*:registry/*",
        "arn:aws:glue:*:*:schema/*"
      ]
    },
    {
      "Sid" : "AllowCompletionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*"
      ]
    },
    {
      "Sid" : "AllowSessionActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/owner" : "${aws:userid}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowGlueTaggingAction",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}",
          "aws:RequestTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowStatementActions",
      "Effect" : "Allow",
      "Action" : [
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:ListStatements",
        "glue:CancelStatement",
        "glue:StopSession",
        "glue:DeleteSession",
        "glue:GetSession"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/owner" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "AllowListSessionsAction",
      "Effect" : "Allow",
      "Action" : [
```

```
        "glue:ListSessions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DenyTagActions",
      "Effect" : "Deny",
      "Action" : [
        "glue:UntagResource",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "owner"
          ]
        }
      }
    },
    {
      "Sid" : "AllowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-glue-*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::aws-glue-*/*",
        "arn:aws:s3:::*/*aws-glue-*/*"
      ]
    },
    {
      "Sid" : "AllowS3ObjectCrawlerActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::crawler-public*"
      ]
    },
    {
      "Sid" : "AllowLogsActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:/aws-glue/*"
      ]
    },
    {
      "Sid" : "AllowTagsActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws-glue-service-resource"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaAccountAdministrator

Beschreibung: Ermöglicht den Zugriff innerhalb von Amazon Grafana zum Erstellen und Verwalten von Arbeitsbereichen für das gesamte Unternehmen.

`AWSGrafanaAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGrafanaAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:20 UTC
- Zeit bearbeitet: 15. Februar 2022, 22:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaAccountAdministrator`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaOrganizationAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMGetRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrafanaIAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "grafana.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaConsoleReadOnlyAccess

Beschreibung: Zugriff auf schreibgeschützte Operationen in Amazon Grafana.

`AWSGrafanaConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGrafanaConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:10 UTC
- Bearbeitete Zeit: 15. Februar 2022, 22:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaConsoleReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "grafana:Describe*",
        "grafana:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaWorkspacePermissionManagement

Beschreibung: Bietet nur die Möglichkeit, Benutzer- und Gruppenberechtigungen für AWS Grafana-Arbeitsbereiche zu aktualisieren.

`AWSGrafanaWorkspacePermissionManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGrafanaWorkspacePermissionManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Februar 2021, 00:15 UTC
- Bearbeitete Zeit: 15. März 2023, 22:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagement`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
```

```
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGrafanaWorkspacePermissionManagementV2

Beschreibung: Bietet die Möglichkeit, Benutzer- und Gruppenberechtigungen für IAM Identity Center (IdC) für Amazon Managed Grafana-Arbeitsbereiche zu aktualisieren.

`AWSGrafanaWorkspacePermissionManagementV2`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSGrafanaWorkspacePermissionManagementV2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2024, 18:39 UTC

- Bearbeitungszeit: 5. Januar 2024, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGrafanaWorkspacePermissionManagementV2`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSGrafanaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:UpdatePermissions",
        "grafana:ListPermissions",
        "grafana:ListWorkspaces"
      ],
      "Resource" : "arn:aws:grafana:*:*:/workspaces*"
    },
    {
      "Sid" : "IAMIdentityCenterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso:ListDirectoryAssociations",
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso-directory:DescribeUser",
```

```
        "sso-directory:DescribeGroup"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die Konfiguration, Verwaltung und Bereitstellung von AWS Greengrass

`AWSGreengrassFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGreengrassFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Mai 2017, 00:47 UTC
- Zeit bearbeitet: 3. Mai 2017, 00:47 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf die AWS Greengrass-Konfiguration, Verwaltung und Bereitstellung

`AWSGreengrassReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGreengrassReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Oktober 2018, 16:01 UTC
- Bearbeitete Zeit: 30. Oktober 2018, 16:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGreengrassReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "greengrass:List*",
        "greengrass:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGreengrassResourceAccessRolePolicy

Beschreibung: Richtlinie für die AWS Greengrass-Dienstrolle, die den Zugriff auf verwandte Dienste wie AWS Lambda und AWS IoT-Ding-Shadows ermöglicht.

`AWSGreengrassResourceAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGreengrassResourceAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Februar 2017, 21:17 UTC
- Zeit bearbeitet: 14. November 2018, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSGreengrassResourceAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowGreengrassAccessToShadows",
      "Action" : [
        "iot:DeleteThingShadow",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iot:*:*:thing/GG_*",
        "arn:aws:iot:*:*:thing/*-gcm",
        "arn:aws:iot:*:*:thing/*-gda",
        "arn:aws:iot:*:*:thing/*-gci"
      ]
    },
    {
      "Sid" : "AllowGreengrassToDescribeThings",
      "Action" : [
        "iot:DescribeThing"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:thing/*"
    },
    {
      "Sid" : "AllowGreengrassToDescribeCertificates",
      "Action" : [
        "iot:DescribeCertificate"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iot:*:*:cert/*"
    },
    {
      "Sid" : "AllowGreengrassToCallGreengrassServices",
      "Action" : [
        "greengrass:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetLambdaFunctions",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassToGetGreengrassSecrets",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Sid" : "AllowGreengrassAccessToS3Objects",
      "Action" : [
        "s3:GetObject"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:s3:::*Greengrass*",
        "arn:aws:s3:::*GreenGrass*",
        "arn:aws:s3:::*greengrass*",
        "arn:aws:s3:::*Sagemaker*",
        "arn:aws:s3:::*SageMaker*",
        "arn:aws:s3:::*sagemaker*"
      ]
    },
    {
      "Sid" : "AllowGreengrassAccessToS3BucketLocation",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGreengrassAccessToSageMakerTrainingJobs",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSGroundStationAgentInstancePolicy

Beschreibung: Stellt der Dataflow Endpoint Instance Berechtigungen zur Verwendung des AWS Ground Station Agents zur Verfügung

`AWSGroundStationAgentInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSGroundStationAgentInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. März 2023, 15:23 UTC
- Bearbeitete Zeit: 20. November 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSGroundStationAgentInstancePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "groundstation:RegisterAgent",
        "groundstation:UpdateAgentStatus",
        "groundstation:GetAgentConfiguration",
        "groundstation:GetAgentTaskResponseUrl"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealth_EventProcessorServiceRolePolicy

Beschreibung: Ermöglicht AWS Health, die Health Event Processor-Funktion zu aktivieren.

`AWSHealth_EventProcessorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Januar 2023, 19:24 UTC
- Bearbeitete Zeit: 13. Januar 2023, 19:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSHealth_EventProcessorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "events:ManagedBy" : "event-processor.health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthFullAccess

Beschreibung: Ermöglicht den vollen Zugriff auf die AWS Health Apis und Benachrichtigungen sowie das Personal Health Dashboard

`AWSHealthFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSHealthFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Dezember 2016, 12:30 Uhr UTC
- Bearbeitete Zeit: 16. November 2020, 18:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "health.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "health:*",
        "organizations:ListAccounts",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "health.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthImagingFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Health Imaging-Service.

`AWSHealthImagingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSHealthImagingFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 23:39 UTC
- Bearbeitete Zeit: 25. Juli 2023, 23:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "medical-imaging.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSHealthImagingReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Health Imaging-Dienst.

`AWSHealthImagingReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSHealthImagingReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Juli 2023, 23:40 UTC
- Bearbeitete Zeit: 1. August 2023, 15:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSHealthImagingReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "medical-imaging:GetDICOMImportJob",
        "medical-imaging:GetDatastore",
        "medical-imaging:GetImageFrame",
        "medical-imaging:GetImageSet",
        "medical-imaging:GetImageSetMetadata",
```

```
        "medical-imaging:ListDICOMImportJobs",
        "medical-imaging:ListDatastores",
        "medical-imaging:ListImageSetVersions",
        "medical-imaging:ListTagsForResource",
        "medical-imaging:SearchImageSets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIAMIdentityCenterAllowListForIdentityContext

Beschreibung: Stellt die Liste der Aktionen bereit, die für Rollen zulässig sind, die im IAM Identity Center-Identitätskontext übernommen wurden. AWS Der Security Token Service (AWS STS) ordnet diese Richtlinie automatisch den übernommenen Rollen zu. Der Identitätskontext wird als ProvidedContext übergeben.

`AWSIAMIdentityCenterAllowListForIdentityContext`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIAMIdentityCenterAllowListForIdentityContext` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 08. November 2023, 15:21 UTC
- Bearbeitete Zeit: 1. Oktober 2024, 14:19 UTC

- ARN: `arn:aws:iam::aws:policy/AWSIAMIdentityCenterAllowListForIdentityContext`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedIdentityPropagation",
      "Effect" : "Deny",
      "NotAction" : [
        "aoss:APIAccessAll",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreatePreparedStatement",
        "athena:DeleteNamedQuery",
        "athena:DeletePreparedStatement",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:UpdateNamedQuery",
```

```
        "athena:UpdatePreparedStatement",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListTableMetadata",
        "athena:ListWorkGroups",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:CancelSteps",
        "elasticmapreduce:DescribeStep",
        "elasticmapreduce:ListSteps",
        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpGet",
        "es:ESHttpPatch",
        "es:ESHttpDelete",
        "es:ESHttpPut",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetTableVersions",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:SearchTables",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchUpdatePartition",
```

```
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "lakeformation:GetDataAccess",
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:StartTroubleshootingAnalysis",
        "q:GetTroubleshootingResults",
        "q:StartTroubleshootingResolutionExplanation",
        "q:UpdateTroubleshootingCommandResult",
        "qapps:CreateQApp",
        "qapps:PredictProblemStatementFromConversation",
        "qapps:PredictQAppFromProblemStatement",
        "qapps:CopyQApp",
        "qapps:GetQApp",
        "qapps:ListQApps",
        "qapps:UpdateQApp",
        "qapps:DeleteQApp",
        "qapps:AssociateQAppWithUser",
        "qapps:DisassociateQAppFromUser",
        "qapps:ImportDocumentToQApp",
        "qapps:ImportDocumentToQAppSession",
        "qapps:CreateLibraryItem",
        "qapps:GetLibraryItem",
        "qapps:UpdateLibraryItem",
        "qapps:CreateLibraryItemReview",
        "qapps:ListLibraryItems",
        "qapps:CreateSubscriptionToken",
        "qapps:StartQAppSession",
        "qapps:StopQAppSession",
        "qapps:PredictQApp",
        "qapps:ImportDocument",
        "qapps:AssociateLibraryItemReview",
        "qapps:DisassociateLibraryItemReview",
        "qapps:GetQAppSession",
        "qapps:UpdateQAppSession",
        "qapps:GetQAppSessionMetadata",
        "qapps:UpdateQAppSessionMetadata",
```

```
        "qapps:TagResource",
        "qapps:ListQAppSessionData",
        "qapps:ExportQAppSessionData",
        "qbusiness:Chat",
        "qbusiness:ChatSync",
        "qbusiness:ListConversations",
        "qbusiness:ListMessages",
        "qbusiness:DeleteConversation",
        "qbusiness:PutFeedback",
        "sts:SetContext"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentityCenterExternalManagementPolicy

Beschreibung: Bietet Zugriff auf die Verwaltung von IAM Identity Center-Benutzern von einem externen Anbieter aus.

`AWSIdentityCenterExternalManagementPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIdentityCenterExternalManagementPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 22. November 2025, 00:34 UTC
- Bearbeitungszeit: 5. Dezember 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIdentityCenterExternalManagementPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IdentityStoreUserCreation",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:CreateUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false",
          "identitystore:ReservedUserId" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "IdentityStoreUserManagement",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:UpdateUser",
        "identitystore:DeleteUser",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/IdentityStoreId}",
        "arn:aws:identitystore:::user/*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "identitystore:UserExternalIdIssuers" : [
            "arn:aws:identitystore::*:identitystore/${aws:PrincipalTag/
IdentityStoreId}/provisioningtenant/${aws:PrincipalTag/IdentityStoreExternalIdIssuer}"
          ]
        },
        "Null" : {
          "identitystore:UserExternalIdIssuers" : "false"
        }
      }
    },
    {
      "Sid" : "IdentityStoreCMKAccess",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : [
            "arn:aws:identitystore::${aws:PrincipalAccount}:identitystore/
${aws:PrincipalTag/IdentityStoreId}"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentitySyncFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Identity Sync-Dienst

`AWSIdentitySyncFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIdentitySyncFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication"
      ],
      "Resource" : "arn:*:ds:*:*:*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile",
        "identity-sync:CreateSyncProfile",
        "identity-sync:GetSyncProfile",
        "identity-sync:StartSync",
        "identity-sync:StopSync",
        "identity-sync:CreateSyncFilter",
        "identity-sync:DeleteSyncFilter",
        "identity-sync:ListSyncFilters",
        "identity-sync:CreateSyncTarget",
        "identity-sync:DeleteSyncTarget",
        "identity-sync:GetSyncTarget",
        "identity-sync:UpdateSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIdentitySyncReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf den Identity Sync-Dienst

`AWSIdentitySyncReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIdentitySyncReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. März 2022, 23:29 UTC
- Bearbeitete Zeit: 23. März 2022, 23:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIdentitySyncReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:GetSyncProfile",
        "identity-sync:ListSyncFilters",
        "identity-sync:GetSyncTarget"
      ],
      "Resource" : "arn:*:identity-sync:*:*:*/*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImageBuilderFullAccess

Beschreibung: Bietet vollen Zugriff auf alle AWS Image Builder Builder-Aktionen und ressourcenspezifischen Zugriff auf zugehörige AWS Dienste.

`AWSImageBuilderFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSImageBuilderFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Dezember 2019, 18:25 Uhr UTC
- Bearbeitete Zeit: 13. April 2021, 17:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:ListLicenseConfigurations",
        "license-manager:ListLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*imagebuilder*",
        "arn:aws:iam::*:role/*imagebuilder*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3::*:*imagebuilder*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "imagebuilder.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ec2:DescribeVolumes",
        "ec2:DescribeSubnets",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImageBuilderReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle AWS Image Builder Builder-Aktionen.

`AWSImageBuilderReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSImageBuilderReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2019, 22:29 Uhr UTC
- Bearbeitete Zeit: 19. Dezember 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImageBuilderReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:Get*",
        "imagebuilder:List*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/imagebuilder.amazonaws.com/
AWSServiceRoleForImageBuilder"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImportExportFullAccess

Beschreibung: Bietet Lese- und Schreibzugriff auf die Jobs, die unter dem erstellt wurden AWS-Konto.

`AWSImportExportFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSImportExportFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSImportExportReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Jobs, die unter dem erstellt wurden AWS-Konto.

`AWSImportExportReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSImportExportReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSImportExportReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "importexport:ListJobs",
        "importexport:GetStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerIncidentAccessServiceRolePolicy

Beschreibung: Erteilt Incident Manager die Berechtigung, im Rahmen der Verwaltung eines Vorfalls andere AWS Dienste aufzurufen.

`AWSIncidentManagerIncidentAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIncidentManagerIncidentAccessServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. November 2023, 00:01 UTC
- Bearbeitete Zeit: 20. Februar 2024, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerIncidentAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "IncidentAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "codedeploy:BatchGetDeployments",
        "codedeploy:ListDeployments",
        "codedeploy:ListDeploymentTargets",
        "autoscaling:DescribeAutoScalingInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerResolverAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Starten, Anzeigen und Aktualisieren von Vorfällen mit vollem Zugriff auf benutzerdefinierte Ereignisse und verwandte Elemente in der Zeitleiste. Weisen Sie diese Richtlinie Benutzern zu, die Vorfälle erstellen und lösen.

`AWSIncidentManagerResolverAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIncidentManagerResolverAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 10. Mai 2021, 06:12 UTC
- Bearbeitete Zeit: 20. November 2025, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIncidentManagerResolverAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "StartIncidentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:StartIncident",
        "ssm-contacts:StartEngagement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResponsePlanReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListResponsePlans",
        "ssm-incidents:GetResponsePlan"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentRecordResolverPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
```

```
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:DeleteTimelineEvent",
        "ssm-incidents:ListRelatedItems",
        "ssm-incidents:UpdateRelatedItems"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIncidentManagerServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Incident Manager die Erlaubnis, Incident-Aufzeichnungen und zugehörige Ressourcen in Ihrem Namen zu verwalten.

`AWSIncidentManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 10. Mai 2021, 03:34 UTC
- Zeit bearbeitet: 28. Januar 2025, 02:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIncidentManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "UpdateIncidentRecordPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-incidents:ListIncidentRecords",
        "ssm-incidents:CreateTimelineEvent"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RelatedOpsItemPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AssociateOpsItemRelatedItem"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IncidentEngagementPermissions",
      "Effect" : "Allow",
      "Action" : "ssm-contacts:StartEngagement",
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IncidentManager",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoT1ClickFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS IoT 1-Click.

`AWSIoT1ClickFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoT1ClickFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2018, 22:10 Uhr UTC

- Bearbeitete Zeit: 11. Mai 2018, 22:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoT1ClickReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS IoT 1-Click.

`AWSIoT1ClickReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoT1ClickReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Mai 2018, 21:49 UTC
- Bearbeitete Zeit: 11. Mai 2018, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoT1ClickReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iot1click:Describe*",
        "iot1click:Get*",
        "iot1click:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTAnalyticsFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT Analytics.

`AWSIoTAnalyticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTAnalyticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2018, 23:02 UTC
- Bearbeitete Zeit: 18. Juni 2018, 23:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTAnalyticsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT Analytics.

`AWSIoTAnalyticsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTAnalyticsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2018, 21:37 UTC
- Bearbeitete Zeit: 18. Juni 2018, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTAnalyticsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotanalytics:Describe*",
        "iotanalytics:List*",
        "iotanalytics:Get*",
        "iotanalytics:SampleChannelData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTConfigAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Konfigurationsaktionen

`AWSIoTConfigAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTConfigAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:52 UTC
- Bearbeitete Zeit: 27. September 2019, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AcceptCertificateTransfer",
        "iot:AddThingToThingGroup",
        "iot:AssociateTargetsWithJob",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CancelCertificateTransfer",
        "iot:CancelJob",
        "iot:CancelJobExecution",
        "iot:ClearDefaultAuthorizer",
```

```
        "iot:CreateAuthorizer",
        "iot:CreateCertificateFromCsr",
        "iot:CreateJob",
        "iot:CreateKeysAndCertificate",
        "iot:CreateOTAUpdate",
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:CreateRoleAlias",
        "iot:CreateStream",
        "iot:CreateThing",
        "iot:CreateThingGroup",
        "iot:CreateThingType",
        "iot:CreateTopicRule",
        "iot:DeleteAuthorizer",
        "iot:DeleteCACertificate",
        "iot:DeleteCertificate",
        "iot:DeleteJob",
        "iot:DeleteJobExecution",
        "iot:DeleteOTAUpdate",
        "iot:DeletePolicy",
        "iot:DeletePolicyVersion",
        "iot:DeleteRegistrationCode",
        "iot:DeleteRoleAlias",
        "iot:DeleteStream",
        "iot:DeleteThing",
        "iot:DeleteThingGroup",
        "iot:DeleteThingType",
        "iot:DeleteTopicRule",
        "iot:DeleteV2LoggingLevel",
        "iot:DeprecateThingType",
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
```

```
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachPrincipalPolicy",
        "iot:DetachThingPrincipal",
        "iot:DisableTopicRule",
        "iot:EnableTopicRule",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
```

```
        "iot:ListV2LoggingLevels",
        "iot:RegisterCACertificate",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RejectCertificateTransfer",
        "iot:RemoveThingFromThingGroup",
        "iot:ReplaceTopicRule",
        "iot:SearchIndex",
        "iot:SetDefaultAuthorizer",
        "iot:SetDefaultPolicyVersion",
        "iot:SetLoggingOptions",
        "iot:SetV2LoggingLevel",
        "iot:SetV2LoggingOptions",
        "iot:StartThingRegistrationTask",
        "iot:StopThingRegistrationTask",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:TransferCertificate",
        "iot:UpdateAuthorizer",
        "iot:UpdateCACertificate",
        "iot:UpdateCertificate",
        "iot:UpdateEventConfigurations",
        "iot:UpdateIndexingConfiguration",
        "iot:UpdateRoleAlias",
        "iot:UpdateStream",
        "iot:UpdateThing",
        "iot:UpdateThingGroup",
        "iot:UpdateThingGroupsForThing",
        "iot:UpdateAccountAuditConfiguration",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DeleteAccountAuditConfiguration",
        "iot:StartOnDemandAuditTask",
        "iot:CancelAuditTask",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:CreateScheduledAudit",
        "iot:UpdateScheduledAudit",
        "iot:DeleteScheduledAudit",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:CreateSecurityProfile",
        "iot:DescribeSecurityProfile",
        "iot:UpdateSecurityProfile",
```

```
        "iot:DeleteSecurityProfile",
        "iot:AttachSecurityProfile",
        "iot:DetachSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTConfigReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf die AWS IoT-Konfigurationsaktionen

`AWSIoTConfigReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTConfigReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:52 Uhr UTC
- Bearbeitete Zeit: 27. September 2019, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTConfigReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeAuthorizer",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:DescribeDefaultAuthorizer",
        "iot:DescribeEndpoint",
        "iot:DescribeEventConfigurations",
        "iot:DescribeIndex",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DescribeRoleAlias",
        "iot:DescribeStream",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingRegistrationTask",
        "iot:DescribeThingType",
        "iot:GetEffectivePolicies",
        "iot:GetIndexingConfiguration",
        "iot:GetJobDocument",
        "iot:GetLoggingOptions",
        "iot:GetOTAUpdate",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:GetRegistrationCode",
        "iot:GetTopicRule",
        "iot:GetV2LoggingOptions",
        "iot:ListAttachedPolicies",
```

```
        "iot:ListAuthorizers",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListCertificatesByCA",
        "iot:ListIndices",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:ListJobs",
        "iot:ListOTAUpdates",
        "iot:ListOutgoingCertificates",
        "iot:ListPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPolicyVersions",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListRoleAliases",
        "iot:ListStreams",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroups",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:ListThingRegistrationTaskReports",
        "iot:ListThingRegistrationTasks",
        "iot:ListThings",
        "iot:ListThingsInThingGroup",
        "iot:ListThingTypes",
        "iot:ListTopicRules",
        "iot:ListV2LoggingLevels",
        "iot:SearchIndex",
        "iot:TestAuthorization",
        "iot:TestInvokeAuthorizer",
        "iot:DescribeAccountAuditConfiguration",
        "iot:DescribeAuditTask",
        "iot:ListAuditTasks",
        "iot:DescribeScheduledAudit",
        "iot:ListScheduledAudits",
        "iot:ListAuditFindings",
        "iot:DescribeSecurityProfile",
        "iot:ListSecurityProfiles",
        "iot:ListSecurityProfilesForTarget",
        "iot:ListTargetsForSecurityProfile",
        "iot:ListActiveViolations",
        "iot:ListViolationEvents",
        "iot:ValidateSecurityProfileBehaviors"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDataAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Messaging-Aktionen

`AWSIoTDataAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDataAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Oktober 2015, 21:51 UTC
- Bearbeitete Zeit: 23. Juni 2021, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDataAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:Connect",
        "iot:Publish",
        "iot:Subscribe",
        "iot:Receive",
        "iot:GetThingShadow",
        "iot:UpdateThingShadow",
        "iot:DeleteThingShadow",
        "iot:ListNamedShadowsForThing"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Dinggruppen und Lesezugriff auf IoT-Zertifikate für die Ausführung von ADD_THINGS_TO_THING_GROUP-Abhilfemaßnahmen

`AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:55 Uhr UTC
- Bearbeitete Zeit: 7. August 2019, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:ListPrincipalThings",
        "iot:AddThingToThingGroup"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderAudit

Beschreibung: Bietet Lesezugriff für IoT und verwandte Ressourcen

`AWSIoTDeviceDefenderAudit`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderAudit` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 18. Juli 2018, 21:17 Uhr UTC
- Bearbeitete Zeit: 25. November 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderAudit`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:GetLoggingOptions",
        "iot:GetV2LoggingOptions",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:DescribeCACertificate",
        "iot:DescribeCertificate",
        "iot:ListPolicies",
        "iot:GetPolicy",
        "iot:GetEffectivePolicies",
        "iot:ListRoleAliases",
        "iot:DescribeRoleAlias",
        "cognito-identity:GetIdentityPoolRoles",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRolePolicy",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetails"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction

Beschreibung: Ermöglicht den Zugriff auf die Aktivierung der IoT-Protokollierung für die Ausführung der ENABLE_IOT_LOGGING-Minderungsaktion

`AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:SetV2LoggingOptions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction

Beschreibung: Ermöglicht die Veröffentlichung von Nachrichten auf das SNS-Thema zur Ausführung der Public_FINDING_TO_SNS-Abhilfemaßnahmen

`AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Richtlinien für die Ausführung von REPLACE_DEFAULT_POLICY_VERSION-Minderungsmaßnahmen

`AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:04 UTC
- Bearbeitete Zeit: 7. August 2019, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderUpdateCACertMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-CA-Zertifikate für die Ausführung von UPDATE_CA_CERTIFICATE-Abhilfemaßnahmen

`AWSIoTDeviceDefenderUpdateCACertMitigationAction`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderUpdateCACertMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:05 UTC
- Bearbeitete Zeit: 7. August 2019, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateCACertMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCACertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction

Beschreibung: Bietet Schreibzugriff auf IoT-Zertifikate für die Ausführung von UPDATE_DEVICE_CERTIFICATE-Abhilfemaßnahmen

`AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 7. August 2019, 17:06 UTC
- Bearbeitete Zeit: 7. August 2019, 17:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceTesterForFreeRTOSFullAccess

Beschreibung: Ermöglicht AWS IoT Device Tester, die FreeRTOS-Qualifizierungssuite auszuführen, indem der Zugriff auf Dienste wie IoT, S3 und IAM ermöglicht wird

`AWSIoTDeviceTesterForFreeRTOSFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceTesterForFreeRTOSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Februar 2020, 20:33 UTC
- Bearbeitete Zeit: 10. August 2023, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForFreeRTOSFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteThing",
        "iot:AttachThingPrincipal",
        "iot:DeleteCertificate",
        "iot:GetRegistrationCode",
```

```
        "iot:CreatePolicy",
        "iot:UpdateCACertificate",
        "s3:ListBucket",
        "iot:DescribeEndpoint",
        "iot:CreateOTAUpdate",
        "iot:CreateStream",
        "signer:ListSigningJobs",
        "acm:ListCertificates",
        "iot:CreateKeysAndCertificate",
        "iot:UpdateCertificate",
        "iot:CreateCertificateFromCsr",
        "iot:DetachThingPrincipal",
        "iot:RegisterCACertificate",
        "iot:CreateThing",
        "iam:ListRoles",
        "iot:RegisterCertificate",
        "iot:DeleteCACertificate",
        "signer:PutSigningProfile",
        "s3:ListAllMyBuckets",
        "signer:ListSigningPlatforms",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "signer:StartSigningJob",
        "acm:GetCertificate",
        "signer:DescribeSigningJob",
        "s3:CreateBucket",
        "execute-api:Invoke",
        "s3:DeleteBucket",
        "s3:PutBucketVersioning",
        "signer:CancelSigningProfile"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
```

```
        "arn:aws:signer:*:*:/signing-profiles/*",
        "arn:aws:signer:*:*:/signing-jobs/*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:acm:*:*:certificate/*",
        "arn:aws:s3:::idt-*",
        "arn:aws:s3:::afr-ota*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteStream",
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy",
        "s3:ListBucketVersions",
        "iot:UpdateCertificate",
        "iot:GetOTAUpdate",
        "iot:DeleteOTAUpdate",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*",
        "arn:aws:iot:*:*:thinggroup/idt*",
        "arn:aws:iam::*:role/idt-*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:DeleteCertificate",
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "s3:DeleteObjectVersion",
        "iot:DeleteOTAUpdate",
        "s3:PutObject",
        "s3:GetObject",
        "iot:DeleteStream",
        "iot:DeletePolicy",
        "s3:DeleteObject",
        "iot:UpdateCertificate",
```

```
        "iot:GetOTAUpdate",
        "s3:GetObjectVersion",
        "iot:DescribeJobExecution"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*",
        "arn:aws:iot:*:*:policy/idt*",
        "arn:aws:iam::*:role/idt-*",
        "arn:aws:iot:*:*:otaupdate/idt*",
        "arn:aws:iot:*:*:thing/idt*",
        "arn:aws:iot:*:*:cert/*",
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:stream/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::afr-ota*/*",
        "arn:aws:s3:::idt-*/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:CancelJobExecution"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/*",
        "arn:aws:iot:*:*:thing/idt*"
      ]
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor10",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "VisualEditor11",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Owner" : "IoTDeviceTester"
        }
      }
    },
    {
      "Sid" : "VisualEditor12",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ssm:DescribeParameters",
        "ssm:GetParameters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor13",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "Owner"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTDeviceTesterForGreengrassFullAccess

Beschreibung: Ermöglicht AWS IoT Device Tester, die AWS Greengrass-Qualifizierungssuite auszuführen, indem der Zugriff auf verwandte Dienste wie Lambda, IoT, API Gateway und IAM ermöglicht wird

`AWSIoTDeviceTesterForGreengrassFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSIoTDeviceTesterForGreengrassFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. Februar 2020, 21:21 UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTDeviceTesterForGreengrassFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor1",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/idt-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "iot.amazonaws.com",
            "lambda.amazonaws.com",
            "greengrass.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "VisualEditor2",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "iot:DeleteCertificate",
        "lambda:DeleteFunction",
        "execute-api:Invoke",
        "iot:UpdateCertificate"
      ],
      "Resource" : [
        "arn:aws:execute-api:us-east-1:098862408343:9xpmnvs5h4/prod/POST/metrics",
        "arn:aws:lambda:*:*:function:idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor3",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor4",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:DetachPolicy",
        "iot:DeletePolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "VisualEditor5",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateJob",
        "iot:DescribeJob",
        "iot:DescribeJobExecution",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:job/*"
      ]
    },
    {
      "Sid" : "VisualEditor6",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "greengrass:*",
        "iam:ListAttachedRolePolicies",
        "iot:CreatePolicy",
        "iot:GetThingShadow",
        "iot:CreateKeysAndCertificate",
        "iot:ListThings",
        "iot:UpdateThingShadow",
        "iot:CreateCertificateFromCsr",
        "iot-device-tester:SendMetrics",
        "iot-device-tester:SupportedVersion",
        "iot-device-tester:LatestIdt",
        "iot-device-tester:CheckVersion",
        "iot-device-tester:DownloadTestSuite"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VisualEditor7",
      "Effect" : "Allow",
      "Action" : [
        "iot:DetachThingPrincipal",
        "iot:AttachThingPrincipal"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/idt-*",
        "arn:aws:iot:*:*:cert/*"
      ]
```

```
    },
    {
      "Sid" : "VisualEditor8",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketVersions",
        "s3:CreateBucket",
        "s3:DeleteObject",
        "s3:DeleteBucket"
      ],
      "Resource" : "arn:aws:s3:::idt*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTEventsFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT Events.

`AWSIoTEventsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTEventsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Januar 2019, 22:51 UTC

- Bearbeitete Zeit: 10. Januar 2019, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTEventsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT Events.

`AWSIoTEventsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTEventsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Januar 2019, 22:50 UTC
- Bearbeitete Zeit: 23. September 2019, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTEventsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotevents:Describe*",
        "iotevents:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFleetHubFederationAccess

Beschreibung: Verbundzugriff für IoT Fleet Hub-Anwendungen

`AWSIoTFleetHubFederationAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTFleetHubFederationAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 15. Dezember 2020, 08:08 UTC
- Bearbeitete Zeit: 4. April 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTFleetHubFederationAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeIndex",
        "iot:DescribeThingGroup",
        "iot:GetBucketsAggregation",
        "iot:GetCardinality",
        "iot:GetIndexingConfiguration",
        "iot:GetPercentiles",
        "iot:GetStatistics",
        "iot:SearchIndex",
        "iot:CreateFleetMetric",
        "iot:ListFleetMetrics",
        "iot:DeleteFleetMetric",
        "iot:DescribeFleetMetric",
        "iot:UpdateFleetMetric",
        "iot:DescribeCustomMetric",
        "iot:ListCustomMetrics",
        "iot:ListDimensions",
        "iot:ListMetricValues",
        "iot:ListThingGroups",
        "iot:ListThingsInThingGroup",
        "iot:ListJobTemplates",
        "iot:DescribeJobTemplate",
        "iot:ListJobs",
        "iot:CreateJob",
        "iot:CancelJob",
        "iot:DescribeJob",
        "iot:ListJobExecutionsForJob",
        "iot:ListJobExecutionsForThing",
        "iot:DescribeJobExecution",
        "iot:ListSecurityProfiles",
        "iot:DescribeSecurityProfile",
        "iot:ListActiveViolations",
        "iot:GetThingShadow",
        "iot:ListNamedShadowsForThing",
        "iot:CancelJobExecution",
        "iot:DescribeEndpoint",
        "iotfleethub:DescribeApplication",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
```

```
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:iotfleethub*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarmHistory"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:iotfleethub*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFleetwiseServiceRolePolicy

Beschreibung: Gewährt Berechtigungen für AWS Ressourcen und Metadaten, die AWSIo TFleetwise für zusätzliche Funktionen verwendet oder verwaltet werden

`AWSIoTFleetwiseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. September 2022, 23:27 UTC
- Bearbeitete Zeit: 16. Oktober 2025, 04:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTFleetwiseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTFleetWise",
```

```
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf die AWS IoT-Konfiguration und die Messaging-Aktionen

`AWSIoTFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. Oktober 2015, 15:19 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2022, 21:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:*",
        "iotjobsdata:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTLogging

Beschreibung: Ermöglicht die Erstellung von Amazon CloudWatch Log-Gruppen und das Streamen von Protokollen an die Gruppen

`AWSIoTLogging`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTLogging` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Oktober 2015, 15:17 Uhr UTC
- Zeit bearbeitet: 8. Oktober 2015, 15:17 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTLogging`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:GetLogEvents",
        "logs:DeleteLogStream"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTManagedIntegrationsFullAccess

Beschreibung: Bietet vollen Zugriff auf verwaltete Integrationen für das AWS IoT Device Management und verwandte Dienste.

`AWSIoTManagedIntegrationsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTManagedIntegrationsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 05. März 2025, 19:22 UTC
- Bearbeitete Zeit: 5. März 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTManagedIntegrationsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotmanagedintegrations:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
iotmanagedintegrations.amazonaws.com/AWSServiceRoleForIoTManagedIntegrations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotmanagedintegrations.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTManagedIntegrationsRolePolicy

Beschreibung: Stellt verwaltete Integrationen für AWS IoT Device Management bereit, um Protokolle und Metriken in Ihrem Namen zu veröffentlichen.

`AWSIoTManagedIntegrationsRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. März 2025, 21:22 UTC
- Bearbeitete Zeit: 5. März 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTManagedIntegrationsRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchStreams",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/iotmanagedintegrations/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : "${aws:ResourceAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/IoTManagedIntegrations",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTOTAUpdate

Beschreibung: Ermöglicht den Zugriff auf die Erstellung eines AWS IoT-Jobs und die Beschreibung des AWS Codesigner-Jobs

`AWSIoTOTAUpdate`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTOTAUpdate` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Dezember 2017, 20:36 Uhr UTC
- Bearbeitete Zeit: 20. Dezember 2017, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTOTAUpdate`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "iot:CreateJob",
      "signer:DescribeSigningJob"
```

```
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf AWS IoT ermöglichen RoboRunner.

`AWSIotRoboRunnerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIotRoboRunnerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 03:54 UTC
- Bearbeitete Zeit: 23. Februar 2023, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iotroborunner:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotroborunner.amazonaws.com/
AWSServiceRoleForIoTRoboRunner",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotroborunner.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerReadOnly

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf IoT ermöglichen. AWS RoboRunner

`AWSIotRoboRunnerReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIotRoboRunnerReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 03:43 UTC
- Zeit bearbeitet: 16. November 2022, 20:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIotRoboRunnerReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotroborunner:GetSite",
        "iotroborunner:GetWorker",
        "iotroborunner:ListWorkerFleets",
        "iotroborunner:ListSites",
        "iotroborunner:ListWorkers",
        "iotroborunner:GetDestination",
        "iotroborunner:GetWorkerFleet",
        "iotroborunner:ListDestinations"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIotRoboRunnerServiceRolePolicy

Beschreibung: Ermöglicht AWS IoT RoboRunner , zugehörige AWS Ressourcen im Namen des Kunden zu verwalten.

`AWSIotRoboRunnerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Februar 2023, 16:56 UTC
- Bearbeitete Zeit: 21. Februar 2023, 16:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIotRoboRunnerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "cloudwatch:PutMetricData"
    ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
        "cloudwatch:namespace" : [
          "AWS/Usage"
        ]
      }
    }
  }
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTRuleActions

Beschreibung: Ermöglicht den Zugriff auf alle AWS Dienste, die in AWS IoT-Regelaktionen unterstützt werden

`AWSIoTRuleActions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTRuleActions` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Oktober 2015, 15:14 Uhr UTC
- Bearbeitete Zeit: 16. Januar 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTRuleActions`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "dynamodb:PutItem",
      "kinesis:PutRecord",
      "iot:Publish",
      "s3:PutObject",
      "sns:Publish",
      "sqs:SendMessage*",
      "cloudwatch:SetAlarmState",
      "cloudwatch:PutMetricData",
      "es:ESHttpPut",
      "firehose:PutRecord"
    ],
    "Resource" : "*"
```

```
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung SiteWise von AWS IoT mithilfe der AWS-Managementkonsole. Beachten Sie, dass diese Richtlinie auch Zugriff auf das Erstellen und Auflisten von mit AWS IoT verwendeten Datenspeichern SiteWise (z. B. AWS IoT Analytics), Zugriff auf das Auflisten und Anzeigen von AWS IoT Greengrass-Ressourcen, das Auflisten und Ändern von AWS Secrets Manager Manager-Geheimnissen, das Abrufen von AWS IoT-Dingschatten, das Auflisten von Ressourcen mit bestimmten Tags und das Erstellen und Verwenden einer dienstbezogenen Rolle für AWS IoT gewährt. SiteWise

`AWSIoTSiteWiseConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTSiteWiseConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Mai 2019, 21:37 UTC
- Bearbeitete Zeit: 31. Mai 2019, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : "iotsitewise:*",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iotanalytics:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Create*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:GetThingShadow"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:ListGroups"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:ListSecrets",
        "secretsmanager:CreateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "secretsmanager:UpdateSecret"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:greengrass-*"
    },
    {
      "Action" : [
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "iotsitewise.amazonaws.com"
        }
      }
    },
    {
      "Action" : [
        "iam:PassRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/iotsitewise.amazonaws.com/
AWSServiceRoleForIoTSiteWise*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "iotsitewise.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseFullAccess

Beschreibung: Bietet vollen Zugriff auf IoT SiteWise.

`AWSIoTSiteWiseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTSiteWiseFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2018, 20:53 UTC
- Bearbeitete Zeit: 4. Dezember 2018, 20:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseMonitorPortalAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen für den Zugriff auf AWS SiteWise IoT-Assets und Asset-Daten, die Erstellung von AWS SiteWise IoT-Monitor-Ressourcen und die Auflistung von AWS SSO-Benutzern.

`AWSIoTSiteWiseMonitorPortalAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTSiteWiseMonitorPortalAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 19. Mai 2020, 20:01 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2020, 20:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTSiteWiseMonitorPortalAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
```

```
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseMonitorServiceRolePolicy

Beschreibung: Diese Rolle gewährt AWS SiteWise IoT-Monitorberechtigungen für den Zugriff auf Ihre AWS SiteWise IoT-Assets und Asset-Eigenschaften sowie für die Erstellung AWS von Sitewise-Projekten, -Dashboards und Zugriffsrichtlinien für AWS IoT über SiteWise IoT-Portale.

`AWSIoTSiteWiseMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2019, 00:59 UTC
- Bearbeitete Zeit: 13. Dezember 2019, 22:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTSiteWiseMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:CreateProject",
        "iotsitewise:DescribeProject",
        "iotsitewise:UpdateProject",
        "iotsitewise:DeleteProject",
        "iotsitewise:ListProjects",
        "iotsitewise:BatchAssociateProjectAssets",
        "iotsitewise:BatchDisassociateProjectAssets",
```

```
        "iotsitewise:ListProjectAssets",
        "iotsitewise:CreateDashboard",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:UpdateDashboard",
        "iotsitewise:DeleteDashboard",
        "iotsitewise:ListDashboards",
        "iotsitewise:CreateAccessPolicy",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:UpdateAccessPolicy",
        "iotsitewise:DeleteAccessPolicy",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:DescribeAsset",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetAssetPropertyAggregates",
        "sso-directory:DescribeUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTSiteWiseReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IoT SiteWise.

`AWSIoTSiteWiseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTSiteWiseReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Dezember 2018, 20:55 UTC
- Zeit bearbeitet: 29. Oktober 2025, 20:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTSiteWiseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:BatchGetAssetPropertyAggregates",
        "iotsitewise:BatchGetAssetPropertyValue",
        "iotsitewise:BatchGetAssetPropertyValueHistory",
        "iotsitewise:DescribeAccessPolicy",
        "iotsitewise:DescribeAction",
        "iotsitewise:DescribeAsset",
        "iotsitewise:DescribeAssetCompositeModel",
        "iotsitewise:DescribeAssetModel",
        "iotsitewise:DescribeAssetModelCompositeModel",
        "iotsitewise:DescribeAssetModelInterfaceRelationship",
        "iotsitewise:DescribeAssetProperty",
        "iotsitewise:DescribeBulkImportJob",
        "iotsitewise:DescribeComputationModel",
        "iotsitewise:DescribeComputationModelExecutionSummary",
        "iotsitewise:DescribeDashboard",
        "iotsitewise:DescribeDataset",
```

```
        "iotsitewise:DescribeDefaultEncryptionConfiguration",
        "iotsitewise:DescribeExecution",
        "iotsitewise:DescribeGateway",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:DescribeLoggingOptions",
        "iotsitewise:DescribePortal",
        "iotsitewise:DescribeProject",
        "iotsitewise:DescribeStorageConfiguration",
        "iotsitewise:DescribeTimeSeries",
        "iotsitewise:ExecuteQuery",
        "iotsitewise:GetAssetPropertyAggregates",
        "iotsitewise:GetAssetPropertyValue",
        "iotsitewise:GetAssetPropertyValueHistory",
        "iotsitewise:GetInterpolatedAssetPropertyValues",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListActions",
        "iotsitewise:ListAssetModelCompositeModels",
        "iotsitewise:ListAssetModelProperties",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssetProperties",
        "iotsitewise:ListAssetRelationships",
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssociatedAssets",
        "iotsitewise:ListBulkImportJobs",
        "iotsitewise:ListCompositionRelationships",
        "iotsitewise:ListComputationModelDataBindingUsages",
        "iotsitewise:ListComputationModelResolveToResources",
        "iotsitewise:ListComputationModels",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListDatasets",
        "iotsitewise:ListExecutions",
        "iotsitewise:ListGateways",
        "iotsitewise:ListInterfaceRelationships",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjectAssets",
        "iotsitewise:ListProjects",
        "iotsitewise:ListTagsForResource",
        "iotsitewise:ListTimeSeries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTThingsRegistration

Beschreibung: Diese Richtlinie ermöglicht es Benutzern, Dinge mithilfe der AWS StartThingRegistrationTask IoT-API massenweise zu registrieren

`AWSIoTThingsRegistration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTThingsRegistration` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2017, 20:21 Uhr UTC
- Bearbeitete Zeit: 5. Oktober 2020, 19:20 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSIoTThingsRegistration`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:AddThingToThingGroup",
        "iot:AttachPolicy",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateCertificateFromCsr",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:DescribeCertificate",
        "iot:DescribeThing",
        "iot:DescribeThingGroup",
        "iot:DescribeThingType",
        "iot:DetachPolicy",
        "iot:DetachThingPrincipal",
        "iot:GetPolicy",
        "iot:ListAttachedPolicies",
        "iot:ListPolicyPrincipals",
        "iot:ListPrincipalPolicies",
        "iot:ListPrincipalThings",
        "iot:ListTargetsForPolicy",
        "iot:ListThingGroupsForThing",
        "iot:ListThingPrincipals",
        "iot:RegisterCertificate",
        "iot:RegisterThing",
        "iot:RemoveThingFromThingGroup",
        "iot:UpdateCertificate",
        "iot:UpdateThing",
        "iot:UpdateThingGroupsForThing",
        "iot:AddThingToBillingGroup",
        "iot:DescribeBillingGroup",
        "iot:RemoveThingFromBillingGroup"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTTwinMakerServiceRolePolicy

Beschreibung: Ermöglicht AWS IoT TwinMaker , andere AWS Dienste anzurufen und deren Ressourcen in Ihrem Namen zu synchronisieren.

`AWSIoTTwinMakerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. November 2023, 18:59 UTC
- Bearbeitete Zeit: 13. November 2023, 18:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIoTTwinMakerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SiteWiseAssetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAsset"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:DescribeAssetModel"
      ],
      "Resource" : [
        "arn:aws:iotsitewise:*:*:asset-model/*"
      ]
    },
    {
      "Sid" : "SiteWiseAssetModelAndAssetListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iotsitewise:ListAssets",
        "iotsitewise:ListAssetModels"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TwinMakerAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetEntity",
        "iottwinmaker:CreateEntity",
        "iottwinmaker:UpdateEntity",
        "iottwinmaker:DeleteEntity",
        "iottwinmaker:ListEntities",
        "iottwinmaker:GetComponentType",
        "iottwinmaker:CreateComponentType",
        "iottwinmaker:UpdateComponentType",
        "iottwinmaker:DeleteComponentType",
        "iottwinmaker:ListComponentTypes"
      ],
      "Resource" : [
        "arn:aws:iottwinmaker:*:*:workspace/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessDataAccess

Beschreibung: Ermöglicht den zugehörigen Identitätsdatenzugriff auf AWS IoT-Wireless-Geräte.

`AWSIoTWirelessDataAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessDataAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:31 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessDataAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:SendDataToWirelessDevice"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessFullAccess

Beschreibung: Ermöglicht der zugehörigen Identität den vollen Zugriff auf alle AWS IoT-Wireless-Operationen.

`AWSIoTWirelessFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:27 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessFullPublishAccess

Beschreibung: Bietet vollen Zugriff auf IoT Wireless, sodass Sie in Ihrem Namen auf der IoT Rules Engine veröffentlichen können.

`AWSIoTWirelessFullPublishAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessFullPublishAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:29 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessFullPublishAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint",
        "iot:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessGatewayCertManager

Beschreibung: Ermöglicht dem zugehörigen Identitätszugriff das Erstellen, Auflisten und Beschreiben von IoT-Zertifikaten

`AWSIoTWirelessGatewayCertManager`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessGatewayCertManager` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:30 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessGatewayCertManager`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IoTWirelessGatewayCertManager",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:DescribeCertificate",
        "iot:ListCertificates"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessLogging

Beschreibung: Ermöglicht der zugehörigen Identität, Amazon CloudWatch Logs-Gruppen zu erstellen und Protokolle an die Gruppen zu streamen.

`AWSIoTWirelessLogging`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessLogging` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:32 Uhr UTC
- Zeit bearbeitet: 15. Dezember 2020, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessLogging`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotwireless*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIoTWirelessReadOnlyAccess

Beschreibung: Ermöglicht der zugehörigen Identität nur Lesezugriff auf AWS IoT-WLAN.

`AWSIoTWirelessReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIoTWirelessReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Dezember 2020, 15:28 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 15:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIoTWirelessReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iotwireless:List*",
        "iotwireless:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIPAMServiceRolePolicy

Beschreibung: Ermöglicht VPC IP Address Manager den Zugriff auf VPC-Ressourcen und die Integration mit AWS Organizations in Ihrem Namen.

`AWSIPAMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2021, 19:08 UTC
- Bearbeitete Zeit: 28. Oktober 2025, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIPAMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "IPAMDiscoveryDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeByoipCidrs",
        "ec2:DescribeIpv6Pools",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:GetIpamDiscoveredAccounts",
        "ec2:GetIpamDiscoveredPublicAddresses",
        "ec2:GetIpamDiscoveredResourceCidrs",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListByoipCidrs",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "cloudfront:ListAnycastIpLists",
        "cloudfront:ListDistributionsByAnycastIpListId",
        "cloudfront:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchMetricsPublishActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/IPAM"
        }
      }
    },
    {
```

```
      "Sid" : "IPAMAllocationPolicyActions",
      "Effect" : "Allow",
      "Action" : "ec2:AllocateIpamPoolCidr",
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListResolverWriteActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyManagedPrefixList"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "Null" : {
          "ec2:Attribute/ExpectedIpamPrefixListResolverTarget" : "false"
        }
      }
    },
    {
      "Sid" : "PrefixListResolverReadActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQContractServiceRolePolicy

Beschreibung: Wird von AWS IQ verwendet, um Zahlungsanforderungen im Namen eines Kunden auszuführen

`AWSIQContractServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. August 2019, 19:28 UTC
- Bearbeitete Zeit: 22. August 2019, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQContractServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:Subscribe"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS IQ

`AWSIQFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSIQFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2019, 23:13 UTC
- Bearbeitete Zeit: 25. September 2019, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSIQFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iq:*",
        "iq-permission:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "permission.iq.amazonaws.com",
            "contract.iq.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSIQPermissionServiceRolePolicy

Beschreibung: Ermöglicht AWS IQ, die von AWS IQ-Experten übernommene Rolle zu verwalten.

`AWSIQPermissionServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. August 2019, 19:36 UTC
- Bearbeitete Zeit: 22. August 2019, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSIQPermissionServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AWSDenyAll"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWSIQPermission-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die für benutzerdefinierte AWS KMS-Schlüsselspeicher erforderlich sind

`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 20:10 UTC
- Bearbeitete Zeit: 10. November 2023, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy

Beschreibung: Ermöglicht AWS KMS, die gemeinsamen Eigenschaften von Schlüsseln mit mehreren Regionen zu synchronisieren.

`AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Juni 2021, 15:37 UTC
- Bearbeitete Zeit: 13. November 2024, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KMSSynchronizeMultiRegionKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:SynchronizeMultiRegionKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSKeyManagementServicePowerUser

Beschreibung: Ermöglicht den Zugriff auf den AWS Key Management Service (KMS).

`AWSKeyManagementServicePowerUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSKeyManagementServicePowerUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC

- Zeit bearbeitet: 7. März 2017, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSKeyManagementServicePowerUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:TagResource",
        "kms:UntagResource",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLakeFormationCrossAccountManager

Beschreibung: Ermöglicht kontenübergreifenden Zugriff auf Glue-Ressourcen über Lake Formation. Gewährt außerdem Lesezugriff auf andere erforderliche Dienste wie Organisationen und den Resource Access Manager

`AWSLakeFormationCrossAccountManager`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLakeFormationCrossAccountManager` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. August 2020, 20:59 UTC
- Bearbeitete Zeit: 25. Februar 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationCrossAccountManager`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceShare",
      "Effect" : "Allow",
      "Action" : [
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManageResourceSharePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceSharePermission"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowXAcctManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PutResourcePolicy",
        "glue:DeleteResourcePolicy",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "ram:Get*",
        "ram:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLakeFormationDataAdmin

Beschreibung: Gewährt administrativen Zugriff auf AWS Lake Formation und verwandte Dienste wie AWS Glue zur Verwaltung von Data Lakes

`AWSLakeFormationDataAdmin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLakeFormationDataAdmin` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. August 2019, 17:33 Uhr UTC
- Bearbeitete Zeit: 03. Dezember 2024, 15:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLakeFormationDataAdmin`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLakeFormationDataAdminAllow",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents",
        "glue:CreateCatalog",
```

```
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:DeleteDatabase",
        "glue:GetConnections",
        "glue:SearchTables",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:GetTableVersions",
        "glue:GetPartitions",
        "glue:GetTables",
        "glue:ListWorkflows",
        "glue:BatchGetWorkflows",
        "glue:DeleteWorkflow",
        "glue:GetWorkflowRuns",
        "glue:StartWorkflowRun",
        "glue:GetWorkflow",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "iam:ListUsers",
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSLakeFormationDataAdminDeny",
      "Effect" : "Deny",
      "Action" : [
        "lakeformation:PutDataLakeSettings"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambda_FullAccess

Beschreibung: Gewährt vollen Zugriff auf den AWS Lambda-Dienst, die Funktionen der AWS Lambda-Konsole und andere zugehörige AWS Dienste.

`AWSLambda_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambda_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2020, 21:14 Uhr UTC
- Bearbeitete Zeit: 1. Dezember 2025, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_FullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "lambda:*",
        "logs:DescribeLogGroups",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lambda.amazonaws.com/
AWSServiceRoleForLambda",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambda_ReadOnlyAccess

Beschreibung: Gewährt schreibgeschützten Zugriff auf den AWS Lambda-Dienst, die Funktionen der AWS Lambda-Konsole und andere verwandte Dienste. AWS

`AWSLambda_ReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSLambda_ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2020, 21:10 Uhr UTC
- Bearbeitete Zeit: 17. März 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambda_ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
```

```
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "lambda:Get*",
        "lambda:List*",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "tag:GetResources",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:DescribeQueries",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaBasicDurableExecutionRolePolicy

Beschreibung: Bietet Schreibberechtigungen für CloudWatch Protokolle und read/write Berechtigungen für die dauerhafte Ausführung, die von dauerhaften Lambda-Funktionen APIs verwendet werden

`AWSLambdaBasicDurableExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaBasicDurableExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 02. Dezember 2025, 15:04 Uhr UTC
- Bearbeitete Zeit: 2. Dezember 2025, 15:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicDurableExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "lambda:CheckpointDurableExecution",
        "lambda:GetDurableExecutionState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaBasicExecutionRole

Beschreibung: Stellt Schreibberechtigungen für CloudWatch Protokolle bereit.

`AWSLambdaBasicExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaBasicExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:03 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 15:03 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaDynamoDBExecutionRole

Beschreibung: Bietet Listen- und Lesezugriff auf DynamoDB-Streams sowie Schreibberechtigungen für Protokolle. CloudWatch

`AWSLambdaDynamoDBExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaDynamoDBExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:09 Uhr UTC
- Bearbeitete Zeit: 9. April 2015, 15:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaENIManagementAccess

Beschreibung: Stellt Mindestberechtigungen für eine Lambda-Funktion zum Verwalten ENIs (Erstellen, Beschreiben, Löschen) bereit, die von einer VPC-fähigen Lambda-Funktion verwendet wird.

`AWSLambdaENIManagementAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSLambdaENIManagementAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2016, 00:37 UTC
- Bearbeitete Zeit: 1. Oktober 2020, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaENIManagementAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaExecute

Beschreibung: Bietet Put, Get Zugriff auf S3 und vollen Zugriff auf CloudWatch Logs.

`AWSLambdaExecute`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaExecute` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaExecute`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:*"
      ],
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaFullAccess

Beschreibung: Diese Richtlinie ist veraltet. Anleitungen finden Sie in der Dokumentation: https:// docs.aws.amazon.com/lambda/ latest/dg/access - control-identity-based .html. Bietet vollen Zugriff auf Lambda, S3, DynamoDB, CloudWatch Metriken und Protokolle.

`AWSLambdaFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSLambdaFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 27. November 2017, 23:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudformation:ListStackResources",
        "cloudwatch:*",
        "cognito-identity:ListIdentityPools",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:SetCognitoEvents",
        "dynamodb:*",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "events:*",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:PassRole",
        "iot:AttachPrincipalPolicy",
        "iot:AttachThingPrincipal",
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy",
        "iot:CreateThing",
        "iot:CreateTopicRule",
        "iot:DescribeEndpoint",
        "iot:GetTopicRule",
        "iot:ListPolicies",
        "iot:ListThings",
        "iot:ListTopicRules",
        "iot:ReplaceTopicRule",
        "kinesis:DescribeStream",
```

```
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:ListAliases",
        "lambda:*",
        "logs:*",
        "s3:*",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Publish",
        "sns:Subscribe",
        "sns:Unsubscribe",
        "sqs:ListQueues",
        "sqs:SendMessage",
        "tag:GetResources",
        "xray:PutTelemetryRecords",
        "xray:PutTraceSegments"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaInvocation-DynamoDB

Beschreibung: Bietet Lesezugriff auf DynamoDB Streams.

`AWSLambdaInvocation-DynamoDB`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaInvocation-DynamoDB` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaInvocation-DynamoDB`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaKinesisExecutionRole

Beschreibung: Bietet Listen- und Lesezugriff auf Kinesis-Streams sowie Schreibberechtigungen für CloudWatch Protokolle.

`AWSLambdaKinesisExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaKinesisExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. April 2015, 15:14 Uhr UTC
- Bearbeitete Zeit: 19. November 2018, 20:09 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamSummary",
        "kinesis:GetRecords",
        "kinesis:GetShardIterator",
        "kinesis:ListShards",
        "kinesis:ListStreams",
        "kinesis:SubscribeToShard",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaManagedEC2ResourceOperator

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Erstellen und Verwalten von EC2 Ressourcen, die von den Lambda Managed Instances verwaltet werden, sowie beschreibende Berechtigungen.

`AWSLambdaManagedEC2ResourceOperator`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSLambdaManagedEC2ResourceOperator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2025, 08:34 UTC
- Zeit bearbeitet: 30. November 2025, 08:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSLambdaManagedEC2ResourceOperator`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateTags",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : "amazon"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaMSKExecutionRole

Beschreibung: Stellt die erforderlichen Berechtigungen für den Zugriff auf den MSK-Cluster innerhalb einer VPC, für die Verwaltung ENIs (Erstellen, Beschreiben, Löschen) in der VPC und für das Schreiben von Berechtigungen für Protokolle bereit. CloudWatch

`AWSLambdaMSKExecutionRole`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSLambdaMSKExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2020, 17:35 Uhr UTC
- Bearbeitete Zeit: 2. August 2022, 20:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaMSKExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2",
        "kafka:GetBootstrapBrokers",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaReplicator

Beschreibung: Gewährt Lambda Replicator die erforderlichen Berechtigungen, um Funktionen regionsübergreifend zu replizieren

`AWSLambdaReplicator`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Mai 2017, 17:53 Uhr UTC
- Zeit bearbeitet: 8. Dezember 2017, 00:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaReplicator`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LambdaCreateDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DisableReplication"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
```

```
    },
    {
      "Sid" : "IamPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFrontListDistributions",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionsByLambdaFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaRole

Beschreibung: Standardrichtlinie für die AWS Lambda-Servicerolle.

`AWSLambdaRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaServiceRolePolicy

Beschreibung: Ermöglicht Lambda, verwaltete Instanzen in Ihrem Namen zu beschreiben und EC2 zu beenden.

`AWSLambdaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2025, 08:04 UTC
- Bearbeitete Zeit: 30. November 2025, 08:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLambdaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ManagedResourceOperator" : "scaler.lambda.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaSQSQueueExecutionRole

Beschreibung: Bietet Zugriff auf SQS-Warteschlangen zum Empfangen von Nachrichten, Löschen von Nachrichten und Lesen von Attributen sowie Schreibberechtigungen für Protokolle. CloudWatch

`AWSLambdaSQSQueueExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaSQSQueueExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Juni 2018, 21:50 Uhr UTC
- Bearbeitete Zeit: 14. Juni 2018, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaSQSQueueExecutionRole`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
```

```
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLambdaVPCAccessExecutionRole

Beschreibung: Stellt Mindestberechtigungen für die Ausführung einer Lambda-Funktion beim Zugriff auf eine Ressource in einer VPC bereit — Netzwerkschnittstellen erstellen, beschreiben, löschen und Schreibberechtigungen für Logs. CloudWatch

`AWSLambdaVPCAccessExecutionRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLambdaVPCAccessExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. Februar 2016, 23:15 Uhr UTC
- Bearbeitete Zeit: 5. Januar 2024, 22:38 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSLambdaVPCAccessExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerConsumptionPolicy

Beschreibung: Stellt Berechtigungen für den Zugriff auf die AWS License Manager API-Aktionen bereit, die für die Nutzung von Lizenzen erforderlich sind, für die der Benutzer berechtigt ist.

`AWSLicenseManagerConsumptionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSLicenseManagerConsumptionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2021, 23:18 Uhr UTC
- Bearbeitete Zeit: 11. August 2021, 23:18 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSLicenseManagerConsumptionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "license-manager:CheckoutLicense",
      "license-manager:CheckInLicense",
```

```
      "license-manager:ExtendLicenseConsumption",
      "license-manager:GetLicense"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

Beschreibung: Ermöglicht dem AWS License Manager Linux Subscriptions Service, Ressourcen in Ihrem Namen zu verwalten.

`AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Dezember 2022, 18:54 UTC
- Bearbeitete Zeit: 8. Juli 2024, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:*"
      ]
    },
    {
      "Sid" : "KMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerMasterAccountRolePolicy

Beschreibung: Rollenrichtlinie für das Masterkonto des AWS License Manager Manager-Dienstes

`AWSLicenseManagerMasterAccountRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:03 UTC
- Bearbeitete Zeit: 31. Mai 2022, 20:50 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMasterAccountRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "S3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*/resource_sync/*"
      ]
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
```

```
        "athena:StartQueryExecution"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetTable",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeAccount",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAccountsForParent",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations",
        "ram:TagResource"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "RAMPermissions3",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/Service" : "LicenseManager"
        }
      }
    },
    {
      "Sid" : "IAMGetRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "IAMPassRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudformationPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/
LicenseManagerCrossAccountCloudDiscoveryStack/*"
      ]
    },
    {
      "Sid" : "GlueUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:UpdateTable",
        "glue:DeleteTable",
        "glue:UpdateJob",
        "glue:UpdateCrawler"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler",
        "arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob",
        "arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*",
        "arn:aws:glue:*:*:table/license_manager_resource_sync/*",
        "arn:aws:glue:*:*:database/license_manager_resource_inventory_db",
        "arn:aws:glue:*:*:database/license_manager_resource_sync"
      ]
    },
    {
      "Sid" : "RGPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:PutGroupPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerMemberAccountRolePolicy

Beschreibung: Rollenrichtlinie für Mitgliedskonten des AWS License Manager Manager-Dienstes

`AWSLicenseManagerMemberAccountRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:04 UTC
- Bearbeitete Zeit: 15. November 2019, 22:09 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerMemberAccountRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:GetLicenseConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:CreateResourceDataSync",
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:ListAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerServiceRolePolicy

Beschreibung: Standardrollenrichtlinie für den AWS License Manager Manager-Dienst

`AWSLicenseManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 19:02 UTC
- Bearbeitete Zeit: 19. November 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/license-
management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "license-management.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPermissionsForCreatingMemberSLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/license-manager.member-
account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "license-manager.member-account.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "S3BucketPermissions1",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "S3BucketPermissions2",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "S3ObjectPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:aws-license-manager-service-*"
      ]
    },
    {
      "Sid" : "SNSTopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeHosts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:ListInventoryEntries",
        "ssm:GetInventory",
        "ssm:CreateAssociation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommandPermission",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*::document/AWSLicenseManager-*"
      ]
    },
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "LicenseManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "license-manager:GetServiceSettings",
        "license-manager:GetLicense*",
        "license-manager:UpdateLicenseSpecificationsForResource",
        "license-manager:List*"
      ],
      "Resource" : [
        "*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

Beschreibung: Ermöglicht dem AWS License Manager User Subscriptions Service, Ressourcen in Ihrem Namen zu verwalten.

`AWSLicenseManagerUserSubscriptionsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. Juli 2022, 01:17 UTC
- Bearbeitete Zeit: 8. November 2024, 02:54 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSLicenseManagerUserSubscriptionsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:GetAuthorizedApplicationDetails"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetInventory",
        "ssm:GetCommandInvocation",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcPeeringConnections"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2WritePermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:TerminateInstances",
        "ec2:CreateTags"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:productCode" : [
            "bz0vcy31ooqlzk5tsash4r1ik",
            "d44g89hc0gp9jdzm99rznthpw",
            "77yzkpa7kvee1y1tt7wnsdwoc",
            "a8jthu9h8pjsn4b8ylvfl6sfr",
            "7at6der8hnlov1g347e6tdkde",
            "3t0v0vuhvxjzm6m462f9v8iz4",
            "4gs2prcp03ojilgkjx8m3ifh7"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SSMDocumentExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunPowerShellScript"
      ]
    },
    {
      "Sid" : "SSMInstanceExecutionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSLicenseManager" : "UserSubscriptions"
        }
      }
```

```
    },
    {
      "Sid" : "ReadHostedZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecurityGroupRulePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "DescribeSubnetsPermissions",
      "Action" : [
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeNetworkInterfacePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:license-manager-user-*"
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSM2ServicePolicy

Beschreibung: Ermöglicht AWS M2, AWS Ressourcen in Ihrem Namen zu verwalten.

`AWSM2ServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Juni 2022, 20:26 UTC
- Bearbeitete Zeit: 7. Juni 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSM2ServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:DescribeFileSystems"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/M2"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_ContactsServiceRolePolicy

Beschreibung: Ermöglicht AWS Managed Services, die Werte der Tags auf AWS Ressourcen zu lesen

`AWSManagedServices_ContactsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. März 2023, 17:07 UTC
- Bearbeitete Zeit: 23. März 2023, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_ContactsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoleTags",
        "iam:ListUserTags",
        "tag:GetResources",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetBucketTagging",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:authType" : "REST-HEADER",
          "s3:signatureversion" : "AWS4-HMAC-SHA256"
        },
        "NumericGreaterThanEquals" : {
          "s3:TlsVersion" : "1.2"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

Beschreibung: AWS Managed Services — Richtlinie zur Verwaltung der Detective Controls-Infrastruktur

`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Dezember 2022, 23:11 UTC
- Zeit bearbeitet: 19. Dezember 2022, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateTermination*",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-recorder",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-config-rules-cdk",
        "arn:aws:cloudformation:*:*:stack/ams-detective-controls-infrastructure-cdk"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeAggregationAuthorizations",
        "config:PutAggregationAuthorization",
        "config:TagResource",
        "config:PutConfigRule"
      ],
      "Resource" : [
        "arn:aws:config:*:*:aggregation-authorization/540708452589/*",
        "arn:aws:config:*:*::config-rule/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:CreateBucket",
        "s3:DeleteBucket",
```

```
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-config-record-bucket-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_EventsServiceRolePolicy

Beschreibung: AWS Managed Services Services-Richtlinie zur Aktivierung der AMS-Ereignisprozessor-Funktion.

`AWSManagedServices_EventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Februar 2023, 18:41 UTC
- Bearbeitete Zeit: 7. Februar 2023, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_EventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "events.managedservices.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServices_SelfServiceReporting_ServiceRolePolicy

Beschreibung: Ermöglicht es der Self Service Reporting-Funktion von Amazon AWS Managed Service, AWS Unternehmensdaten in Ihrem Namen zu lesen, um aggregierte Berichte auf Organisationsebene zu ermöglichen

`AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 8. Januar 2025, 21:22 UTC
- Bearbeitete Zeit: 8. Januar 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServices_SelfServiceReporting_ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeAccount",
        "organizations:ListAccounts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagedServicesDeploymentToolkitPolicy

Beschreibung: Ermöglicht AWS Managed Services, das Deployment Toolkit in Ihrem Namen zu verwalten.

`AWSManagedServicesDeploymentToolkitPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Juni 2022, 18:33 UTC
- Bearbeitete Zeit: 4. April 2024, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSManagedServicesDeploymentToolkitPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AMSCDKToolkitS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObject",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObjectVersionTagging",
```

```
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketVersioning",
        "s3:GetLifecycleConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectAttributes",
        "s3:GetObjectLegalHold",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionTorrent",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutBucketAcl",
        "s3:PutBucketLogging",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::ams-cdktoolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitCloudFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:GetTemplate",
```

```
        "cloudformation:GetTemplateSummary",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateTerminationProtection"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*"
    },
    {
      "Sid" : "AMSCDKToolkitECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:CreateRepository",
        "ecr:DeleteLifecyclePolicy",
        "ecr:DeleteRepository",
        "ecr:DeleteRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:ListTagsForResource",
        "ecr:PutImageScanningConfiguration",
        "ecr:PutImageTagMutability",
        "ecr:PutLifecyclePolicy",
        "ecr:SetRepositoryPolicy",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/ams-cdktoolkit*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagementConsoleAdministratorAccess

Beschreibung: Bietet vollen Zugriff zur Konfiguration und Anpassung der AWS-Managementkonsole

`AWSManagementConsoleAdministratorAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSManagementConsoleAdministratorAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 14. August 2025, 21:19 UTC
- Bearbeitete Zeit: 10. Dezember 2025, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/AWSManagementConsoleAdministratorAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
        "uxc:PutAccountColor",
        "uxc:DeleteAccountColor",
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:AssociateChannel",
        "notifications:AssociateManagedNotificationAccountContact",
        "notifications:AssociateManagedNotificationAdditionalChannel",
```

```
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DeregisterNotificationHub",
        "notifications:DisableNotificationsAccessForOrganization",
        "notifications:DisassociateChannel",
        "notifications:DisassociateManagedNotificationAccountContact",
        "notifications:DisassociateManagedNotificationAdditionalChannel",
        "notifications:EnableNotificationsAccessForOrganization",
        "notifications:GetEventRule",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListManagedNotificationChannelAssociations",
        "notifications:ListManagedNotificationChildEvents",
        "notifications:ListManagedNotificationConfigurations",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:RegisterNotificationHub",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:DeleteEnvironment",
        "cloudshell:GetFileDownloadUrls",
        "cloudshell:GetFileUploadUrls",
        "cloudshell:DescribeEnvironments",
        "cloudshell:PutCredentials",
        "cloudshell:StartEnvironment",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
```

```
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSManagementConsoleBasicUserAccess

Beschreibung: Gewährt Benutzern ohne Administratorrechte Zugriff auf wichtige AWS-Managementkonsole Funktionen und Funktionen zur Benutzererfahrung (UX).

`AWSManagementConsoleBasicUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSManagementConsoleBasicUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2025, 20:34 UTC
- Bearbeitete Zeit: 10. Dezember 2025, 00:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSManagementConsoleBasicUserAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "uxc:GetAccountColor",
```

```
        "ec2:DescribeRegions",
        "notifications:GetFeatureOptInStatus",
        "notifications:ListManagedNotificationEvents",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationEvents",
        "notifications:ListNotificationHubs",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationEvent",
        "notifications:ListManagedNotificationChildEvents",
        "cloudshell:CreateEnvironment",
        "cloudshell:CreateSession",
        "cloudshell:GetEnvironmentStatus",
        "cloudshell:StartEnvironment",
        "cloudshell:DeleteEnvironment",
        "cloudshell:PutCredentials",
        "cloudshell:StopEnvironment",
        "cloudshell:ApproveCommand",
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search",
        "action-recommendations:ListRecommendedActions",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceAmiIngestion

Beschreibung: Ermöglicht AWS Marketplace das Kopieren Ihrer Amazon Machine Images (AMIs), um sie aufzulisten AWS Marketplace

`AWSMarketplaceAmiIngestion`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceAmiIngestion` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. September 2020, 20:55 UTC
- Bearbeitete Zeit: 25. September 2020, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceAmiIngestion`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:ec2:us-east-1::snapshot/snap-*"
    },
```

```
    {
      "Action" : [
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshotAttribute",
        "ec2:ModifyImageAttribute"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceDeploymentServiceRolePolicy

Beschreibung: Ermöglicht AWS Marketplace die Erstellung und Verwaltung von Verkäufer-Deployment-Parametern für die Produkte, die Sie abonnieren AWS Marketplace.

`AWSMarketplaceDeploymentServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 23:34 UTC
- Bearbeitete Zeit: 15. November 2023, 23:34 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceDeploymentServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ManageMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:RemoveRegionsFromReplication"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:marketplace-deployment*!*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagMarketplaceDeploymentSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:marketplace-deployment!*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/expirationDate" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "expirationDate"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceFullAccess

Beschreibung: Ermöglicht das Abonnieren und Abbestellen von AWS Marketplace Software, ermöglicht Benutzern die Verwaltung von Marketplace-Softwareinstanzen über die Marketplace-Seite „Ihre Software“ und bietet Administratorzugriff auf. EC2

`AWSMarketplaceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Februar 2015, 17:21 Uhr UTC
- Bearbeitete Zeit: 7. Mai 2025, 20:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcs",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DeregisterImage",
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeInstanceStatus",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "sns:ListTopics",
        "sns:GetTopicAttributes",
        "sns:CreateTopic",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:ListRoles",
        "iam:ListInstanceProfiles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceGetEntitlements

Beschreibung: Bietet Lesezugriff auf AWS Marketplace Berechtigungen

`AWSMarketplaceGetEntitlements`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceGetEntitlements` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2017, 19:37 UTC
- Bearbeitete Zeit: 5. April 2024, 01:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceGetEntitlements`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceGetEntitlements",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetEntitlements"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceImageBuildFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Marketplace Private Image Build-Funktion. Neben der Erstellung privater Images bietet es auch Berechtigungen zum Hinzufügen von Tags zu Images sowie zum Starten und Beenden von EC2-Instances.

`AWSMarketplaceImageBuildFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceImageBuildFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Juli 2018, 23:29 Uhr UTC
- Bearbeitete Zeit: 4. März 2022, 17:05 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceImageBuildFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListBuilds",
        "aws-marketplace:StartBuild",
        "aws-marketplace:DescribeBuilds"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/marketplace-image-build:build-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*Automation*",
        "arn:aws:iam::*:role/*Instance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:DescribeDocument",
        "ec2:DeregisterImage",
        "ec2:CopyImage",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DeleteSnapshot",
        "ec2:CreateImage",
        "ec2:RunInstances",
        "ec2:DescribeInstanceStatus",
        "sns:GetTopicAttributes",
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:*image-build*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
        "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
        "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
        "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
        "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
        "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
        "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
        "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:eu-central-1:906690553262:automation-definition/*",
            "arn:aws:ssm:us-east-1:058657716661:automation-definition/*",
            "arn:aws:ssm:ap-northeast-1:340648487307:automation-definition/*",
            "arn:aws:ssm:eu-west-1:564714592864:automation-definition/*",
            "arn:aws:ssm:us-west-2:243045473901:automation-definition/*",
            "arn:aws:ssm:ap-southeast-2:362149219987:automation-definition/*",
            "arn:aws:ssm:eu-west-2:587945719687:automation-definition/*",
            "arn:aws:ssm:us-east-2:134937423163:automation-definition/*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/marketplace-image-build:build-id" : "*"
        },
        "StringNotEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceLicenseManagementServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die AWS Marketplace für die Lizenzverwaltung verwendet oder verwaltet werden.

`AWSMarketplaceLicenseManagementServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2020, 08:33 UTC
- Bearbeitete Zeit: 3. Dezember 2020, 08:33 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceLicenseManagementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowLicenseManagerActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "license-manager:ListReceivedGrants",
        "license-manager:ListDistributedGrants",
        "license-manager:GetGrant",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager:DeleteGrant",
        "license-manager:AcceptGrant"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceManageSubscriptions

Beschreibung: Ermöglicht das Abonnieren und Abbestellen von AWS Marketplace Software

`AWSMarketplaceManageSubscriptions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceManageSubscriptions` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 1. Dezember 2025, 00:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceManageSubscriptions`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:UpdatePurchaseOrders",
        "aws-marketplace:ListAgreementCharges",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
        "aws-marketplace:AcceptAgreementPaymentRequest",
        "aws-marketplace:RejectAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        },
        "Null" : {
          "aws-marketplace:AgreementType" : "false"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
    },
```

```
    {
      "Sid" : "AWSMarketplaceTokenManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AgentTokenContainer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "CreateAgentTokenContainer",
            "RequestExpressPrivateOffer",
            "ExpireToken"
          ]
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceEntityReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceMeteringFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Marketplace Metering.

`AWSMarketplaceMeteringFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceMeteringFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. März 2016, 22:39 Uhr UTC
- Bearbeitete Zeit: 17. März 2016, 22:39 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:MeterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceMeteringRegisterUsage

Beschreibung: Stellt Berechtigungen zur Registrierung einer Ressource und zur Nachverfolgung der Nutzung über den AWS Marketplace Messdienst bereit.

`AWSMarketplaceMeteringRegisterUsage`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceMeteringRegisterUsage` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. November 2019, 01:17 UTC
- Zeit bearbeitet: 21. November 2019, 01:17 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceMeteringRegisterUsage`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "aws-marketplace:RegisterUsage"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceProcurementSystemAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf alle administrativen Aktionen für eine AWS Marketplace eProcurement-Integration.

`AWSMarketplaceProcurementSystemAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceProcurementSystemAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 25. Juni 2019, 13:07 UTC
- Bearbeitete Zeit: 25. Juni 2019, 13:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceProcurementSystemAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutProcurementSystemConfiguration",
        "aws-marketplace:DescribeProcurementSystemConfiguration",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplacePurchaseOrdersServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff von AWS Marketplace Diensten auf die Bestellverwaltung.

`AWSMarketplacePurchaseOrdersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. Oktober 2021, 15:12 Uhr UTC
- Bearbeitete Zeit: 27. Oktober 2021, 15:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplacePurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowPurchaseOrderActions",
      "Effect" : "Allow",
      "Action" : [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceRead-only

Beschreibung: Bietet die Möglichkeit, AWS Marketplace Abonnements zu überprüfen

`AWSMarketplaceRead-only`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceRead-only` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Zeit bearbeitet: 1. Dezember 2025, 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceRead-only`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:ListAgreementCharges",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListInstanceProfiles",
        "sns:GetTopicAttributes",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListPrivateListings"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceResaleAuthorizationServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von AWS Marketplace for Resale Authorization verwendet oder verwaltet werden.

`AWSMarketplaceResaleAuthorizationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. März 2024, 18:47 UTC

- Zeit bearbeitet: 1. August 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMarketplaceResaleAuthorizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMCreate",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:RequestedResourceType" : "aws-marketplace:Entity"
        },
        "ArnLike" : {
          "ram:ResourceArn" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
        },
        "Null" : {
          "ram:Principal" : "true"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAssociate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "Null" : {
          "ram:Principal" : "false"
        },
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMAcceptDelete",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:DeleteResourceShare"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "AWSMarketplaceResaleAuthorization"
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsRAMGet",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : [
        "arn:aws:ram:*:*:*"
      ]
    },
    {
```

```
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplace",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowResaleAuthorizationShareActionsMarketplaceDescribe",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:*/ResaleAuthorization/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerFullAccess

Beschreibung: Bietet vollen Zugriff auf alle Verkäufervorgänge AWS Marketplace und andere AWS Dienste wie AMI-Management.

`AWSMarketplaceSellerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceSellerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 20:40 UTC
- Zeit bearbeitet: 1. Dezember 2025, 00:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerFullAccess`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:uploadFiles",
        "aws-marketplace-management:viewReports",
        "aws-marketplace-management:viewSupport",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:GetSellerDashboard",
        "aws-marketplace:ListAssessments",
```

```
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AgreementAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "AssetScanning",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsights",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "SellerSettings",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace-management:GetSellerVerificationDetails",
        "aws-marketplace-management:PutSellerVerificationDetails",
        "aws-marketplace-management:GetBankAccountVerificationDetails",
        "aws-marketplace-management:PutBankAccountVerificationDetails",
        "aws-marketplace-management:GetSecondaryUserVerificationDetails",
        "aws-marketplace-management:PutSecondaryUserVerificationDetails",
        "aws-marketplace-management:GetAdditionalSellerNotificationRecipients",
        "aws-marketplace-management:PutAdditionalSellerNotificationRecipients",
        "payments:GetPaymentInstrument",
        "payments:CreatePaymentInstrument",
        "tax:GetTaxInterview",
        "tax:PutTaxInterview",
```

```
        "tax:GetTaxInfoReportingDocument",
        "tax:ListSupplementalTaxRegistrations",
        "tax:PutSupplementalTaxRegistration",
        "tax:DeleteSupplementalTaxRegistration",
        "tax:GetTaxRegistration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Support",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourcePolicyManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "resale-authorization.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AgreementPaymentRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SendAgreementPaymentRequest",
        "aws-marketplace:GetAgreementPaymentRequest",
        "aws-marketplace:ListAgreementPaymentRequests",
```

```
        "aws-marketplace:CancelAgreementPaymentRequest"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerOfferManagement

Beschreibung: Bietet Verkäufern Zugriff auf Aktivitäten zur Verwaltung von Angeboten und Vereinbarungen.

`AWSMarketplaceSellerOfferManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceSellerOfferManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 19. November 2024, 00:41 UTC
- Zeit bearbeitet: 19. November 2024, 00:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerOfferManagement`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSMarketplaceChangeSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceOfferManagement",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceCreateOfferOnProduct",
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : "CreateOfferOnProduct"
        }
      }
    },
    {
      "Sid" : "AWSMarketplaceListEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntitiesReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Offer/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ContainerProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProfessionalServicesProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/SaaSProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/AmiProduct/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ResaleAuthorization/*"
      ]
    },
    {
      "Sid" : "AWSMarketplaceAgreementsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:DescribeAgreement",
        "aws-marketplace:GetAgreementTerms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws-marketplace:PartyType" : "Proposer"
        },
        "ForAllValues:StringEquals" : {
          "aws-marketplace:AgreementType" : [
            "PurchaseAgreement"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsFullAccess

Beschreibung: Bietet Verkäufern vollen Zugriff auf die AWS Marketplace Management-Produktseite und andere AWS Dienste wie AMI-Management.

`AWSMarketplaceSellerProductsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceSellerProductsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 21:06 UTC
- Bearbeitete Zeit: 1. Dezember 2025, 00:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MarketplaceListAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListAssessments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MarketplaceResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:CancelChangeSet",
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceAssessmentAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeAssessment"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "EC2ResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:ModifyImageAttribute",
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetIAMRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "IAMPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "assets.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "VendorInsightsAccess",
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "ResourceSharingAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy",
        "aws-marketplace:PutResourcePolicy",
        "aws-marketplace:DeleteResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace*/*"
    },
    {
      "Sid" : "MarketplaceEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-files/
${aws:PrincipalAccount}/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "TechnicalStaff"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMarketplaceSellerProductsReadOnly

Beschreibung: Bieten Sie Verkäufern nur Lesezugriff auf die Seite mit AWS Marketplace Verwaltungsprodukten.

`AWSMarketplaceSellerProductsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMarketplaceSellerProductsReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Juli 2019, 21:40 Uhr UTC
- Bearbeitete Zeit: 10. Dezember 2024, 18:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMarketplaceSellerProductsReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:ListAssessments",
        "aws-marketplace:DescribeAssessment",
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:GetResourcePolicy"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMcpServiceActionsFullAccess

Beschreibung: Bietet vollen Zugriff auf alle MCP-Serviceaktionen. Diese Richtlinie gewährt keinen Zugriff auf die vom MCP ausgeführten Aktionen, sondern nur auf die MCP-Aktionen selbst.

`AWSMcpServiceActionsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMcpServiceActionsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. November 2025, 22:49 UTC
- Bearbeitete Zeit: 21. November 2025, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMcpServiceActionsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowAllMCPServiceActions",
      "Effect" : "Allow",
      "Action" : "*",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:IsMcpServiceAction" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMediaConnectServicePolicy

Beschreibung: Die Standardrichtlinie, die den Zugriff AWS-Services auf Ressourcen ermöglicht, die von verwendet oder verwaltet werden MediaConnect.

`AWSMediaConnectServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. April 2023, 22:11 UTC
- Bearbeitete Zeit: 29. Oktober 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaConnectServicePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService",
        "ecs:CreateService",
        "ecs:DescribeServices",
        "ecs:PutAttributes",
        "ecs:DeleteAttributes",
        "ecs:RunTask",
        "ecs:ListTasks",
        "ecs:StartTask",
        "ecs:StopTask",
        "ecs:DescribeTasks",
        "ecs:DescribeContainerInstances",
        "ecs:UpdateContainerInstancesState"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:UpdateClusterSettings",
        "ecs:ListAttributes",
        "ecs:DescribeClusters",
        "ecs:DeregisterContainerInstance",
        "ecs:ListContainerInstances"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/MediaConnectGateway"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/created-for-service" : "MediaConnect"
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMediaLiveAnywhereServiceRolePolicy

Beschreibung: Ermöglicht MediaLive Anywhere, AWS Ressourcen in Ihrem Namen zu erstellen und zu verwalten.

`AWSMediaLiveAnywhereServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. April 2025, 22:07 UTC
- Bearbeitete Zeit: 14. April 2025, 22:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaLiveAnywhereServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PutMediaLiveMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MediaLive"
        }
      }
    },
    {
      "Sid" : "RegisterAnywhereAgentTaskDefinition",
      "Effect" : "Allow",
      "Action" : [
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        }
      }
    },
    {
      "Sid" : "ECSTagResource",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:TagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ecs:CreateAction" : "RegisterTaskDefinition",
          "aws:RequestTag/created_by" : "MediaLiveAnywhere"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "created_by"
        }
      }
    },
    {
      "Sid" : "UpdateAnywhereAgentService",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*",
          "ecs:Task-Definition" : "arn:aws:ecs:*:*:task-definition/
MediaLiveAnywhereAgent*"
        }
      }
    },
    {
      "Sid" : "ECSListTaskDefinitions",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListTaskDefinitions"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "DeregisterAnywhereAgentTaskDefinitionOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeregisterTaskDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentTaskDefinitionsOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteTaskDefinitions"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:task-definition/MediaLiveAnywhereAgent*"
      ]
    },
    {
      "Sid" : "DeleteAnywhereAgentServiceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteService"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:service/MediaLiveAnywhere*/MediaLiveAnywhereAgent*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ecs:Cluster" : "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
        }
      }
    },
    {
      "Sid" : "DeregisterContainerInstanceOnCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListContainerInstances",
        "ecs:DeregisterContainerInstance"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/MediaLiveAnywhere*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMediaTailorServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die verwendet oder verwaltet werden von MediaTailor

`AWSMediaTailorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. September 2021, 22:27 UTC
- Bearbeitete Zeit: 17. September 2021, 22:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMediaTailorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:MediaTailor/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubDiscoveryAccess

Beschreibung: Die Richtlinie AWSMigration HubService ermöglicht es, AWSApplication DiscoveryService im Namen des Kunden anzurufen.

`AWSMigrationHubDiscoveryAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubDiscoveryAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:30 Uhr UTC
- Bearbeitete Zeit: 6. August 2020, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDiscoveryAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubDMSAccess

Beschreibung: Richtlinie für den Database Migration Service, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`AWSMigrationHubDMSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubDMSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 14:00 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubDMSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
```

```
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubFullAccess

Beschreibung: Verwaltete Richtlinie, um dem Kunden Zugriff auf den Migration Hub Service zu gewähren

`AWSMigrationHubFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. August 2017, 14:02 UTC
- Bearbeitete Zeit: 19. Juni 2019, 21:14 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:*",
        "discovery:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:GetRole"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "continuousexport.discovery.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
continuousexport.discovery.amazonaws.com/
AWSServiceRoleForApplicationDiscoveryServiceContinuousExport*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "migrationhub.amazonaws.com",
            "dmsintegration.migrationhub.amazonaws.com",
            "smsintegration.migrationhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorConsoleFullAccess

Beschreibung: Bietet eingeschränkten Zugriff auf AWS Migration Hub, AWS Application Discovery Service, Amazon Simple Storage Service und AWS Secrets Manager. Diese Richtlinie gewährt auch vollen Zugriff auf den AWS Migration Hub Orchestrator-Dienst.

`AWSMigrationHubOrchestratorConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubOrchestratorConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2022, 02:26 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHO",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "S3MHO",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "ListSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Configuration",
      "Effect" : "Allow",
      "Action" : [
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations",
        "discovery:GetDiscoverySummary"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetHomeRegion",
      "Effect" : "Allow",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListProfileRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListInstanceProfiles",
        "iam:ListRoles"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:ListClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Account",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateServiceRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-orchestrator.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSServiceRoleForMigrationHubOrchestrator*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorInstanceRolePolicy

Beschreibung: Diese Richtlinie muss für SAP- und MGN-migrierte Instanzen angehängt werden, damit unser Service Instanzen orchestrieren kann, indem er Skripts von S3 herunterlädt und geheime Werte innerhalb der Instanz abruft. EC2

`AWSMigrationHubOrchestratorInstanceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubOrchestratorInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2022, 02:43 UTC
- Bearbeitete Zeit: 20. April 2022, 02:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorPlugin

Beschreibung: Bietet eingeschränkten Zugriff auf Amazon Simple Storage Service, AWS Secrets Manager und Plugin-bezogene Aktionen für AWS Migration Hub Orchestrator.

`AWSMigrationHubOrchestratorPlugin`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubOrchestratorPlugin` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. April 2022, 02:25 UTC
- Bearbeitete Zeit: 20. April 2022, 02:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubOrchestratorPlugin`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-orchestrator-*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-orchestrator:RegisterPlugin",
        "migrationhub-orchestrator:GetMessage",
        "migrationhub-orchestrator:SendMessage"
      ],
      "Resource" : "arn:aws:migrationhub-orchestrator:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubOrchestratorServiceRolePolicy

Beschreibung: Stellt die erforderlichen Berechtigungen für Migration Hub Orchestrator bereit, um Ihre lokalen Workloads zu migrieren und zu modernisieren

`AWSMigrationHubOrchestratorServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. April 2022, 02:24 UTC
- Bearbeitete Zeit: 4. März 2024, 18:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubOrchestratorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationDiscoveryService",
      "Effect" : "Allow",
      "Action" : [
```

```
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LaunchWizard",
      "Effect" : "Allow",
      "Action" : [
        "launchwizard:ListProvisionedApps",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:ListDeployments",
        "launchwizard:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2MGNLaunchTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged" : "mgn.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ec2LaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeLaunchTemplates"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "getHomeRegion",
      "Action" : [
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Sid" : "SSMcommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:CancelCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:s3:::aws-migrationhub-orchestrator-*",
        "arn:aws:s3:::migrationhub-orchestrator-*"
      ]
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "s3GetObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::migrationhub-orchestrator-*",
```

```
        "arn:aws:s3:::migrationhub-orchestrator-*/*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DescribeRule",
        "events:DeleteRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
    },
    {
      "Sid" : "MGN",
      "Effect" : "Allow",
      "Action" : [
        "mgn:GetReplicationConfiguration",
        "mgn:GetLaunchConfiguration",
        "mgn:StartCutover",
        "mgn:FinalizeCutover",
        "mgn:StartTest",
        "mgn:UpdateReplicationConfiguration",
        "mgn:DescribeSourceServers",
        "mgn:MarkAsArchived",
        "mgn:ChangeServerLifeCycleState"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ec2DescribeImportImage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImportImageTasks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "s3ListBucket",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
```

```
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "migrationhub-orchestrator-vmie-*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS Migration Hub Refactor Spaces und andere AWS zugehörige Dienste mit Ausnahme von AWS Transit Gateway und EC2 Sicherheitsgruppen, die bei der Verwendung von Umgebungen ohne Netzwerkbrücke nicht erforderlich sind. Diese Richtlinie schließt auch Berechtigungen aus, die für AWS Lambda und AWS Resource Access Manager erforderlich sind, da sie anhand von Tags eingeschränkt werden können.

`AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. April 2023, 20:09 UTC
- Bearbeitete Zeit: 11. April 2024, 18:16 UTC

- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpaces-EnvironmentsWithoutBridgesFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagsDelete",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
```

```
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
```

```
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
```

```
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpaces-SSMAutomationPolicy

Beschreibung: Wird in der IAM-Dienstrolle verwendet, die an das SSM-Automatisierungsdokument übergeben wurde, AWSRefactorSpaces-CreateResources um die für die Ausführung der Automatisierung erforderlichen Berechtigungen zu gewähren. Die Richtlinie gewährt read/write Zugriff auf EC2 Tags, um den Automatisierungsfortschritt zu verfolgen. Wenn die Netzwerkbrücke der Refactor Spaces-Umgebung aktiviert ist, fügt die Automatisierung der EC2 Instanz auch die Sicherheitsgruppe der Umgebung hinzu, um Datenverkehr von anderen Refactor Spaces-Diensten in der Umgebung zuzulassen. Die Richtlinie gewährt auch Zugriff auf die SSM-Parameter für Aktionen nach dem Start des Application Migration Service.

`AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubRefactorSpaces-SSMAutomationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. August 2023, 15:08 UTC
- Bearbeitete Zeit: 10. August 2023, 15:08 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubRefactorSpaces-SSMAutomationPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/refactor-spaces:ssm:optin" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "refactor-spaces:ssm:environment-id"
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-
*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesFullAccess

Beschreibung: Gewährt vollen Zugriff auf AWS MigrationHub Refactor Spaces, AWS MigrationHub Refactor Spaces-Konsolenfunktionen und andere verwandte AWS Dienste, mit Ausnahme der für AWS Lambda und AWS Resource Access Manager erforderlichen Berechtigungen, da diese basierend auf Tags eingeschränkt werden können.

`AWSMigrationHubRefactorSpacesFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubRefactorSpacesFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2021, 07:12 Uhr UTC
- Bearbeitete Zeit: 11. April 2024, 17:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubRefactorSpacesFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RefactorSpaces",
      "Effect" : "Allow",
      "Action" : [
        "refactor-spaces:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcs",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RequestTagTransitGatewayCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "ResourceTagTransitGatewayCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGateway",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTransitGatewayVpcAttachment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2NetworkingModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTransitGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
```

```
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Sid" : "VpcEndpointServiceConfigurationDelete",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBDescribe",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeListeners"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ELBModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Sid" : "ELBLoadBalancerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
    {
      "Sid" : "ELBListenerCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "ELBListenerDelete",
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Sid" : "ELBTargetGroupModify",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Sid" : "ELBTargetGroupCreate",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayModify",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:DELETE",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT",
        "apigateway:UpdateRestApiPolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Sid" : "APIGatewayVpcLinksGet",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "OrganizationDescribe",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudformationStackTag",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:TagResource"
```

```
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/*"
    },
    {
      "Sid" : "CreateRefactorSpacesSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "refactor-spaces.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateELBSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubRefactorSpacesServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Ressourcen, die von AWS Migration Hub Refactor Spaces verwaltet oder verwendet werden.

`AWSMigrationHubRefactorSpacesServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2021, 06:50 UTC
- Bearbeitete Zeit: 20. Juli 2023, 15:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubRefactorSpacesServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:DeleteTags",
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:environment-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:DeleteVpcEndpointServiceConfigurations",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:CreateListener",
        "elasticloadbalancing:DeleteListener",
```

```
        "elasticloadbalancing:DeleteTargetGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/refactor-spaces:route-id" : [
            "*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:PUT",
        "apigateway:POST",
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/vpclinks/*",
        "arn:aws:apigateway:*::/tags",
        "arn:aws:apigateway:*::/tags/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:application-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : "arn:aws:apigateway:*::/vpclinks/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteLoadBalancer",
      "Resource" : "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-
nlb-*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "arn:*:elasticloadbalancing:*:*:loadbalancer/net/refactor-spaces-nlb-*",
        "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:DeleteListener",
      "Resource" : "arn:*:elasticloadbalancing:*:*:listener/net/refactor-spaces-nlb-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:RegisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeregisterTargets"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/refactor-spaces:route-id" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : "arn:*:elasticloadbalancing:*:*:targetgroup/refactor-spaces-tg-*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/refactor-spaces:route-id" : "false"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubSMSAccess

Beschreibung: Richtlinie für den Servermigrationsdienst, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`AWSMigrationHubSMSAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubSMSAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. August 2017, 13:57 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:01 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMigrationHubSMSAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "mgh:CreateProgressUpdateStream"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Action" : [
        "mgh:AssociateCreatedArtifact",
        "mgh:DescribeMigrationTask",
        "mgh:DisassociateCreatedArtifact",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:AssociateDiscoveredResource",
        "mgh:DisassociateDiscoveredResource",
        "mgh:ListDiscoveredResources"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/*"
    },
    {
      "Action" : [
        "mgh:ListMigrationTasks",
```

```
        "mgh:GetHomeRegion"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyCollector

Beschreibung: Erteilt Berechtigungen zur Kommunikation mit dem AWS Migration Hub Strategy Recommendations Service, read/write Zugriff auf S3-Buckets im Zusammenhang mit dem Service, Amazon API Gateway Gateway-Zugriff zum Hochladen von Logs und Metriken AWS, AWS Secrets Manager Manager-Zugriff zum Abrufen von Anmeldeinformationen und alle zugehörigen Dienste.

`AWSMigrationHubStrategyCollector`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubStrategyCollector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Oktober 2021, 20:15 Uhr UTC
- Bearbeitete Zeit: 1. April 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyCollector`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MHSRAllowS3Resources",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowS3ListBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MHSRAllowMetricsAndLogs",
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:PutMetricData",
        "application-transformation:PutLogData",
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "MHSRAllowExecuteAPI",
      "Effect" : "Allow",
      "Action" : [
        "execute-api:Invoke",
        "execute-api:ManageConnections"
      ],
      "Resource" : [
        "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
        "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
      ]
    },
    {
      "Sid" : "MHSRAllowCollectorAPI",
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:RegisterCollector",
        "migrationhub-strategy:GetAntiPattern",
        "migrationhub-strategy:GetMessage",
        "migrationhub-strategy:SendMessage",
        "migrationhub-strategy:ListAntiPatterns",
        "migrationhub-strategy:ListJarArtifacts",
        "migrationhub-strategy:UpdateCollectorConfiguration",
        "migrationhub-strategy:PutLogData",
        "migrationhub-strategy:PutMetricData"
```

```
      ],
      "Resource" : "arn:aws:migrationhub-strategy:*:*:*"
    },
    {
      "Sid" : "MHSRAllowSecretsManager",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:migrationhub-strategy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyConsoleFullAccess

Beschreibung: Gewährt vollen Zugriff auf den Service AWS Migration Hub Strategy Recommendations und Zugriff auf verwandte AWS Dienste über die AWS-Managementkonsole.

`AWSMigrationHubStrategyConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMigrationHubStrategyConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Oktober 2021, 20:13 UTC
- Bearbeitete Zeit: 9. November 2022, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMigrationHubStrategyConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "migrationhub-strategy:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:CreateBucket",
```

```
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:GetDiscoverySummary",
        "discovery:DescribeTags",
        "discovery:DescribeConfigurations",
        "discovery:ListConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "migrationhub-strategy.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/migrationhub-
strategy.amazonaws.com/AWSMigrationHubStrategyServiceRolePolicy*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMigrationHubStrategyServiceRolePolicy

Beschreibung: Ermöglichen Sie den Zugriff auf AWS Ressourcen, die vom AWS Migration Hub Strategy Recommendations Service verwendet oder verwaltet werden.

`AWSMigrationHubStrategyServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Oktober 2021, 20:02 UTC
- Bearbeitete Zeit: 19. Oktober 2021, 20:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSMigrationHubStrategyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "permissionsForAds",
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
        "discovery:DescribeConfigurations",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "permissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource" : "arn:aws:s3:::migrationhub-strategy-*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMobileHub_FullAccess

Beschreibung: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu erteilen, Projekte (und die zugehörigen AWS Ressourcen) in AWS Mobile Hub zu erstellen, zu löschen und zu ändern. Dazu gehören auch Berechtigungen zum Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt.

`AWSMobileHub_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMobileHub_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2016, 19:56 UTC
- Bearbeitete Zeit: 19. Dezember 2019, 23:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_FullAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "apigateway:POST",
        "cloudfront:GetDistribution",
        "devicefarm:CreateProject",
        "devicefarm:ListJobs",
        "devicefarm:ListRuns",
        "devicefarm:GetProject",
        "devicefarm:GetRun",
        "devicefarm:ListArtifacts",
        "devicefarm:ListProjects",
        "devicefarm:ScheduleRun",
        "dynamodb:DescribeTable",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
```

```
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*-mobilehub-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMobileHub_ReadOnly

Beschreibung: Diese Richtlinie kann an jeden Benutzer, jede Rolle oder Gruppe angehängt werden, um Benutzern die Erlaubnis zu erteilen, Projekte in AWS Mobile Hub aufzulisten und anzusehen. Dazu gehören auch Berechtigungen zum Generieren und Herunterladen von Beispielquellcode für mobile Apps für jedes Mobile Hub Hub-Projekt. Es erlaubt dem Benutzer nicht, die Konfiguration für ein Mobile Hub Hub-Projekt zu ändern.

`AWSMobileHub_ReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSMobileHub_ReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Januar 2016, 19:55 UTC
- Bearbeitete Zeit: 23. Juli 2018, 21:59 UTC
- ARN: `arn:aws:iam::aws:policy/AWSMobileHub_ReadOnly`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "iam:ListSAMLProviders",
        "lambda:ListFunctions",
        "sns:ListTopics",
        "lex:GetIntent",
        "lex:GetIntents",
        "lex:GetSlotType",
        "lex:GetSlotTypes",
        "lex:GetBot",
        "lex:GetBots",
        "lex:GetBotAlias",
        "lex:GetBotAliases",
        "mobilehub:ExportProject",
        "mobilehub:GenerateProjectParameters",
        "mobilehub:GetProject",
        "mobilehub:SynchronizeProject",
```

```
        "mobilehub:GetProjectSnapshot",
        "mobilehub:ListProjectSnapshots",
        "mobilehub:ListAvailableConnectors",
        "mobilehub:ListAvailableFeatures",
        "mobilehub:ListAvailableRegions",
        "mobilehub:ListProjects",
        "mobilehub:ValidateProject",
        "mobilehub:VerifyServiceRole",
        "mobilehub:DescribeBundle",
        "mobilehub:ExportBundle",
        "mobilehub:ListBundles"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/aws-my-sample-app*.zip"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSMSKReplicatorExecutionRole

Beschreibung: Erteilt Amazon MSK Replicator die Erlaubnis, Daten zwischen MSK-Clustern zu replizieren.

`AWSMSKReplicatorExecutionRole`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSMSKReplicatorExecutionRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Dezember 2023, 00:07 Uhr UTC
- Bearbeitete Zeit: 25. März 2024, 21:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSMSKReplicatorExecutionRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ClusterPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:Connect",
        "kafka-cluster:DescribeCluster",
        "kafka-cluster:AlterCluster",
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup",
```

```
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:WriteDataIdempotently"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "TopicPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:DescribeTopic",
        "kafka-cluster:CreateTopic",
        "kafka-cluster:AlterTopic",
        "kafka-cluster:WriteData",
        "kafka-cluster:ReadData",
        "kafka-cluster:DescribeTopicDynamicConfiguration",
        "kafka-cluster:AlterTopicDynamicConfiguration",
        "kafka-cluster:AlterCluster"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:topic/*/*"
      ]
    },
    {
      "Sid" : "GroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kafka-cluster:AlterGroup",
        "kafka-cluster:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:kafka:*:*:group/*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNATGatewayServiceRolePolicy

Beschreibung: Stellt Berechtigungen zur Verwaltung von VPC-Ressourcen für die Konfiguration und Verwaltung von NAT-Gateways bereit.

`AWSNATGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2025, 17:19 UTC
- Bearbeitete Zeit: 14. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNATGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkFirewallFullAccess

Beschreibung: Gewährt vollen Zugriff auf den AWS Netzwerk-Firewall-Dienst, einschließlich der Berechtigungen zum Erstellen, Konfigurieren, Verwalten und Löschen von Firewall-Ressourcen, Richtlinien und Regelgruppen. Enthält außerdem Berechtigungen zum Ändern von VPC-Endpunkten, S3-Bucket-Richtlinien, CloudWatch Protokollkonfigurationen und zum Erstellen von dienstbezogenen Rollen für Network Firewall und Log-Delivery-Dienste

`AWSNetworkFirewallFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSNetworkFirewallFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Juni 2025, 21:52 UTC

- Bearbeitete Zeit: 10. Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "NetworkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "network-firewall:AssociateFirewallPolicy",
```

```
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:CreateRuleGroup",
        "network-firewall:CreateTLSInspectionConfiguration",
        "network-firewall:DeleteFirewall",
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DeleteRuleGroup",
        "network-firewall:DeleteTLSInspectionConfiguration",
        "network-firewall:DisassociateSubnets",
        "network-firewall:PutResourcePolicy",
        "network-firewall:StartAnalysisReport",
        "network-firewall:StartFlowCapture",
        "network-firewall:StartFlowFlush",
        "network-firewall:UpdateFirewallAnalysisSettings",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallDescription",
        "network-firewall:UpdateFirewallEncryptionConfiguration",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:UpdateRuleGroup",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:UpdateTLSInspectionConfiguration"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*"
      ]
    },
    {
      "Sid" : "NetworkFirewallEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallCreateVpcEndpoint",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallDeleteVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogging",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallLoggingCWL",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallLoggingS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLoggingFirehose",
      "Effect" : "Allow",
      "Action" : "firehose:TagDeliveryStream",
      "Resource" : "arn:aws:firehose:*:*:*"
    },
    {
      "Sid" : "NetworkFirewallSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/network-firewall.amazonaws.com/
AWSServiceRoleForNetworkFirewall"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "network-firewall.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "NetworkFirewallLogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkFirewallReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Netzwerk-Firewall-Ressourcen über die AWS-Managementkonsole CLI und. SDKs Mit dieser Richtlinie können Benutzer Firewallkonfigurationen, Richtlinien, Regelgruppen und zugehörige Ressourcen anzeigen und überwachen, ohne Änderungen vornehmen zu können.

`AWSNetworkFirewallReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSNetworkFirewallReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Juni 2025, 21:52 UTC
- Bearbeitete Zeit: 10. Juni 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkFirewallReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListAnalysisReports",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListFlowOperations",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTagsForResource",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeFlowOperation",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:GetAnalysisReportResults",
        "network-firewall:ListFlowOperationResults"
      ],
      "Resource" : "arn:aws:network-firewall:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkFirewallServiceRolePolicy

Beschreibung: Erlauben Sie der AWSNetwork Firewall, die erforderlichen Ressourcen für Ihre Firewalls zu erstellen und zu verwalten.

`AWSNetworkFirewallServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2020, 17:17 Uhr UTC
- Bearbeitete Zeit: 30. März 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkFirewallServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "acm:DescribeCertificate",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "resource-groups:ListGroupResources",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "resource-groups.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AWSNetworkFirewallManaged" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerCloudWANServiceRolePolicy

Beschreibung: Erlauben Sie NetworkManager den Zugriff auf Ressourcen, die mit Ihrem Kernnetzwerk verknüpft sind

`AWSNetworkManagerCloudWANServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juli 2022, 12:17 UTC
- Bearbeitete Zeit: 12. Juli 2022, 12:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerCloudWANServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTransitGatewayRouteTableAnnouncement",
        "ec2:DeleteTransitGatewayRouteTableAnnouncement",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:DisableTransitGatewayRouteTablePropagation"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon NetworkManager über die AWS-Managementkonsole.

`AWSNetworkManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSNetworkManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2019, 17:37 UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "networkmanager:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "networkmanager.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerReadOnlyAccess

Beschreibung: Bietet Nur-Lesezugriff auf Amazon NetworkManager über die AWS-Managementkonsole.

`AWSNetworkManagerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSNetworkManagerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 3. Dezember 2019, 17:35 Uhr UTC
- Bearbeitete Zeit: 3. Dezember 2019, 17:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSNetworkManagerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:Describe*",
        "networkmanager:Get*",
        "networkmanager:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSNetworkManagerServiceRolePolicy

Beschreibung: Erlauben Sie den NetworkManager Zugriff auf Ressourcen, die Ihren globalen Netzwerken zugeordnet sind

`AWSNetworkManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 14:03 UTC
- Bearbeitete Zeit: 27. Juli 2022, 19:41 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSNetworkManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeLocations",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpcs",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeRegions",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:GetTransitGatewayPolicyTableAssociations",
        "ec2:GetTransitGatewayPolicyTableEntries"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSObservabilityAdminLogsCentralizationServiceRolePolicy

Beschreibung: Dienstbezogene Rollenberechtigungen für die Zentralisierung von CloudWatch Protokollen

`AWSObservabilityAdminLogsCentralizationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. September 2025, 14:34 UTC
- Bearbeitete Zeit: 15. September 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminLogsCentralizationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "logs.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/LogsManaged" : "true"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:logs:arn" : "arn:aws:logs:*:*:log-group:*"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSObservabilityAdminServiceRolePolicy

Beschreibung: Bietet Zugriff auf die Verwaltung von AWS Config Configuration Recorder, die Verwaltung des AWS Config Configuration Aggregators, die Erstellung einer mit dem AWS Config Service verknüpften Rolle für die Configuration Recorder-Funktionalität, die Nutzung von Recorder-Konfigurationsdaten und das Lesen von AWS Organisationsdaten für Organisationsfunktionen.

`AWSObservabilityAdminServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2024, 19:36 UTC
- Bearbeitete Zeit: 27. November 2024, 19:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigurationAggregator",
        "config:DeleteConfigurationAggregator",
        "config:SelectAggregateResourceConfig"
      ],
      "Resource" : [
        "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
observabilityadmin.amazonaws.com/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "config.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "observabilityadmin.amazonaws.com",
            "config.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSObservabilityAdminTelemetryEnablementServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf die Verwaltung der Ressourcen- und Telemetrieeinstellungen für AWS Config Recorder für AWS Ressourcen wie Protokolle und Metriken.

`AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. August 2025, 18:04 UTC

- Zeit bearbeitet: 2. Dezember 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSObservabilityAdminTelemetryEnablementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TelemetryOperations",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeFlowLogs",
        "ec2:DescribeVpcs",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "logs:ListLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagOperationForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ec2:CreateAction" : "CreateFlowLogs"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TagOperationForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForVPCFlowLogs",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateFlowLogs"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-flow-log/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchTelemetryRuleManaged"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteFlowLogs",
        "logs:CreateDelivery",
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliverySource",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSApiLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/api" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuditLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/audit" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSAuthenticatorLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/authenticator" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSControllerManagerLogs",
      "Effect" : "Allow",
```

```
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/controllerManager" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForEKSSchedulerLogs",
      "Effect" : "Allow",
      "Action" : [
        "eks:UpdateClusterConfig"
      ],
      "Resource" : "arn:aws:eks:*:*:cluster/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Bool" : {
          "eks:loggingType/scheduler" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLoggingConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "arn:aws:wafv2:*:*:regional/webacl/*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:logs:*:*:log-group:*"
        },
        "StringEquals" : {
          "wafv2:LogScope" : "CloudwatchTelemetryRuleManaged",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TelemetryOperationsForWafLogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForELB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "bedrock-agentcore:AllowVendedLogDeliveryForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "TelemetryOperationsForCloudTrailLogs",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/cloudwatch/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForManagedLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:PutResourcePolicy",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/cloudtrail",
        "arn:aws:logs:*:*:log-group:aws/cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingListOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingGetOperations",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigCreation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:CreateResolverQueryLogConfig",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:resolver-query-log-config/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Route53QueryLoggingConfigAssociation",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateResolverQueryLogConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CloudWatchTelemetryRuleManaged" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDeliverySLR",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/route53resolver.amazonaws.com/
AWSServiceRoleForRoute53Resolver",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "route53resolver.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "TelemetryOperationsForRoute53LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMOperationsForConfigServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "config.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "BoolIfExists" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "ManagementOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForObservabilityAdmin_TelemetryEnablement/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadOperationsForServiceLinkedRecorder",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "config:ConfigurationRecorderServicePrincipal" : [
            "telemetry-enablement.observabilityadmin.amazonaws.com"
          ],
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Organizations.

`AWSOrganizationsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSOrganizationsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. November 2018, 20:31 UTC
- Bearbeitete Zeit: 22. April 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsFullAccess",
      "Effect" : "Allow",
      "Action" : "organizations:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:PutAlternateContact",
        "account:DeleteAlternateContact",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:PutContactInformation",
        "account:ListRegions",
        "account:EnableRegion",
        "account:DisableRegion",
        "account:PutAccountName",
        "account:GetAccountInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsFullAccessCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "organizations.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsReadOnlyAccess

Beschreibung: Bietet Nur-Lese-Zugriff für Organizations. AWS

`AWSOrganizationsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSOrganizationsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. November 2018, 20:32 UTC
- Bearbeitete Zeit: 7. Juni 2024, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSOrganizationsReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSOrganizationsReadOnlyAccount",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "account:GetPrimaryEmail"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOrganizationsServiceTrustPolicy

Beschreibung: Eine Richtlinie, die es AWS Organizations ermöglicht, Vertrauen mit anderen zu teilen, die genehmigt wurde AWS-Services , um die Kundenkonfiguration zu vereinfachen.

`AWSOrganizationsServiceTrustPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Oktober 2017, 23:04 UTC
- Bearbeitete Zeit: 1. November 2017, 06:01 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOrganizationsServiceTrustPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForOrganizations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/organizations.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOutpostsAuthorizeServerPolicy

Beschreibung: Diese Richtlinie gewährt Ihnen Berechtigungen, mit denen Sie einen Outpost-Server in Ihrem lokalen Netzwerk installieren können.

`AWSOutpostsAuthorizeServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSOutpostsAuthorizeServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 4. Januar 2023, 19:23 UTC
- Bearbeitete Zeit: 4. Januar 2023, 19:23 UTC
- ARN: `arn:aws:iam::aws:policy/AWSOutpostsAuthorizeServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSOutpostsServiceRolePolicy

Beschreibung: Richtlinie für dienstverknüpfte Rollen, um den Zugriff auf AWS Ressourcen zu ermöglichen, die von AWS Outposts verwaltet werden

`AWSOutpostsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2020, 22:55 UTC
- Bearbeitete Zeit: 17. April 2025, 17:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSOutpostsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateConnectivityServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfacePolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*",
        "arn:*:ec2:*:*:subnet/*",
        "arn:*:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateNetworkInterfaceTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:vpc/*"
```

```
      ]
    },
    {
      "Sid" : "PrivateConnectivityCreateSecurityGroupTaggingPolicy",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "outposts:private-connectivity-resourceId"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaApplianceRolePolicy

Beschreibung: Ermöglicht der AWS IoT-Software auf einer AWS Panorama-Appliance, Protokolle auf Amazon hochzuladen CloudWatch.

`AWSPanoramaApplianceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaApplianceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:13 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*"
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/panorama_device*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaApplianceServiceRolePolicy

Beschreibung: Ermöglicht einer AWS Panorama-Appliance CloudWatch, Protokolle auf Amazon hochzuladen und Objekte von Amazon S3 S3-Zugriffspunkten abzurufen, die für die Verwendung mit AWS Panorama erstellt wurden.

`AWSPanoramaApplianceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaApplianceServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Oktober 2021, 12:14 Uhr UTC
- Bearbeitete Zeit: 10. Dezember 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaApplianceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaDeviceCreateLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDeviceCreateLogGroup",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
      ]
    },
    {
      "Sid" : "PanoramaDevicePutMetric",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "PanoramaDeviceMetrics"
        }
      }
    },
    {
      "Sid" : "PanoramaDeviceS3Access",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3:::*-nodepackage-store-*",
        "arn:aws:s3:::*-application-payload-store-*",
        "arn:aws:s3:*:*:accesspoint/panorama*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Panorama

`AWSPanoramaFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2020, 13:12 UTC
- Bearbeitete Zeit: 10. Dezember 2024, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPanoramaFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
```

```
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/panorama*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "panorama.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/panorama_device*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/panorama/devices/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "panorama.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaGreengrassGroupRolePolicy

Beschreibung: Ermöglicht einer AWS Lambda-Funktion auf einer AWS Panorama-Appliance, Ressourcen in Panorama zu verwalten, Protokolle und Metriken auf Amazon hochzuladen und Objekte in Buckets zu verwalten CloudWatch, die für die Verwendung mit Panorama erstellt wurden.

`AWSPanoramaGreengrassGroupRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaGreengrassGroupRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:10 Uhr UTC
- Bearbeitete Zeit: 6. Januar 2021, 19:30 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaGreengrassGroupRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCLoudWatchPutDashboard",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutDashboard",
      "Resource" : [
        "arn:aws:cloudwatch::*:dashboard/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaCloudWatchPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*"
    },
    {
      "Sid" : "PanoramaGreenGrassCloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/greengrass/*"
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:*"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaSageMakerRolePolicy

Beschreibung: Ermöglicht Amazon SageMaker , Objekte in Buckets zu verwalten, die für die Verwendung mit AWS Panorama erstellt wurden.

`AWSPanoramaSageMakerRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaSageMakerRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:13 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:13 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaSageMakerRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaSageMakerS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:GetBucket*"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaServiceLinkedRolePolicy

Beschreibung: Ermöglicht AWS Panorama die Verwaltung von Ressourcen in AWS IoT, AWS Secrets Manager und AWS Panorama.

`AWSPanoramaServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Oktober 2021, 12:12 Uhr UTC
- Bearbeitete Zeit: 20. Oktober 2021, 12:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPanoramaServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
```

```
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateKeysAndCertificate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyAndVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicy",
        "iot:CreatePolicyVersion",
        "iot:AttachPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
```

```
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "panorama:Describe*",
        "panorama:List*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : [
```

```
        "arn:aws:secretsmanager:*:*:secret:panorama*",
        "arn:aws:secretsmanager:*:*:secret:Panorama*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPanoramaServiceRolePolicy

Beschreibung: Ermöglicht AWS Panorama, Ressourcen in Amazon S3, AWS IoT, AWS IoT GreenGrass, AWS Lambda SageMaker, Amazon und Amazon CloudWatch Logs zu verwalten und Servicerollen an AWS IoT GreenGrass, AWS IoT und Amazon SageMaker zu übergeben.

`AWSPanoramaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPanoramaServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Dezember 2020, 13:14 Uhr UTC
- Zeit bearbeitet: 1. Dezember 2020, 13:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSPanoramaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PanoramaIoTThingAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreateThing",
        "iot:DeleteThing",
        "iot:DeleteThingShadow",
        "iot:DescribeThing",
        "iot:GetThingShadow",
        "iot:UpdateThing",
        "iot:UpdateThingShadow"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCertificateAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachThingPrincipal",
        "iot:DetachThingPrincipal",
        "iot:UpdateCertificate",
        "iot:DeleteCertificate",
        "iot:AttachPrincipalPolicy",
        "iot:DetachPrincipalPolicy"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:thing/panorama*",
        "arn:aws:iot:*:*:cert/*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreateCertificateAndPolicyAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iot:CreateKeysAndCertificate",
        "iot:CreatePolicy"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaIoTCreatePolicyVersionAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:CreatePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeJobExecution",
        "iot:CreateJob",
        "iot:DeleteJob"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:job/panorama*",
        "arn:aws:iot:*:*:thing/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIoTEndpointAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:DescribeEndpoint"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "panorama:Describe*",
        "panorama:List*",
        "panorama:Get*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:DeleteBucket",
        "s3:ListBucket",
        "s3:GetBucket*",
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*aws-panorama*"
      ]
    },
    {
      "Sid" : "PanoramaIAMPassSageMakerRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaSageMakerRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaSageMakerRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "PanoramaIAMPassGreengrassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassGroupRole",
        "arn:aws:iam::*:role/AWSPanoramaGreengrassRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaGreengrassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "greengrass.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PanoramaIAMPassIoTRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPanoramaApplianceRole",
        "arn:aws:iam::*:role/service-role/AWSPanoramaApplianceRole"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "iot.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PanoramaGreenGrassAccess",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:AssociateRoleToGroup",
        "greengrass:AssociateServiceRoleToAccount",
        "greengrass:CreateResourceDefinition",
        "greengrass:CreateResourceDefinitionVersion",
        "greengrass:CreateCoreDefinition",
```

```
        "greengrass:CreateCoreDefinitionVersion",
        "greengrass:CreateDeployment",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:CreateGroup",
        "greengrass:CreateGroupCertificateAuthority",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateLoggerDefinition",
        "greengrass:CreateLoggerDefinitionVersion",
        "greengrass:CreateSubscriptionDefinition",
        "greengrass:CreateSubscriptionDefinitionVersion",
        "greengrass:DeleteCoreDefinition",
        "greengrass:DeleteFunctionDefinition",
        "greengrass:DeleteResourceDefinition",
        "greengrass:DeleteGroup",
        "greengrass:DeleteLoggerDefinition",
        "greengrass:DeleteSubscriptionDefinition",
        "greengrass:DisassociateRoleFromGroup",
        "greengrass:DisassociateServiceRoleFromAccount",
        "greengrass:GetAssociatedRole",
        "greengrass:GetConnectivityInfo",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetDeviceDefinition",
        "greengrass:GetDeviceDefinitionVersion",
        "greengrass:GetFunctionDefinition",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupCertificateAuthority",
        "greengrass:GetGroupCertificateConfiguration",
        "greengrass:GetGroupVersion",
        "greengrass:GetLoggerDefinition",
        "greengrass:GetLoggerDefinitionVersion",
        "greengrass:GetResourceDefinition",
        "greengrass:GetServiceRoleForAccount",
        "greengrass:GetSubscriptionDefinition",
        "greengrass:GetSubscriptionDefinitionVersion",
        "greengrass:ListCoreDefinitionVersions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeployments",
        "greengrass:ListDeviceDefinitionVersions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitionVersions",
```

```
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroupCertificateAuthorities",
        "greengrass:ListGroupVersions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitionVersions",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListSubscriptionDefinitionVersions",
        "greengrass:ListSubscriptionDefinitions",
        "greengrass:ResetDeployments",
        "greengrass:UpdateConnectivityInfo",
        "greengrass:UpdateCoreDefinition",
        "greengrass:UpdateDeviceDefinition",
        "greengrass:UpdateFunctionDefinition",
        "greengrass:UpdateGroup",
        "greengrass:UpdateGroupCertificateConfiguration",
        "greengrass:UpdateLoggerDefinition",
        "greengrass:UpdateSubscriptionDefinition",
        "greengrass:UpdateResourceDefinition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaLambdaUsersFunctionAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:DescribeCompilationJob",
```

```
        "sagemaker:StopCompilationJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/panorama*",
        "arn:aws:sagemaker:*:*:compilation-job/panorama*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerListAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCompilationJobs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PanoramaSageMakerReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:training-job/*"
      ]
    },
    {
      "Sid" : "PanoramaCWLogsAccess",
      "Effect" : "Allow",
      "Action" : [
        "iot:AttachPolicy",
        "iot:CreateRoleAlias"
      ],
      "Resource" : [
        "arn:aws:iot:*:*:policy/panorama*",
        "arn:aws:iot:*:*:rolealias/panorama*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralChannelHandshakeApprovalManagement

Beschreibung: Stellt den erforderlichen Zugriff für die Verwaltung der Kanalhandshake-Genehmigung bereit.

`AWSPartnerCentralChannelHandshakeApprovalManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralChannelHandshakeApprovalManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. November 2025, 16:34 UTC
- Bearbeitete Zeit: 19. November 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelHandshakeApprovalManagement`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelHandshakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListChannelHandshakes",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralChannelManagement

Beschreibung: Stellt den erforderlichen Zugriff für Channel-Management-Aktivitäten bereit.

`AWSPartnerCentralChannelManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralChannelManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. November 2025, 16:34 UTC
- Bearbeitete Zeit: 1. Dezember 2025, 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralChannelManagement`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ChannelManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateProgramManagementAccount",
        "partnercentral:UpdateProgramManagementAccount",
        "partnercentral:DeleteProgramManagementAccount",
        "partnercentral:ListProgramManagementAccounts",
        "partnercentral:GetProgramManagementAccount",
        "partnercentral:CreateRelationship",
        "partnercentral:UpdateRelationship",
        "partnercentral:DeleteRelationship",
        "partnercentral:GetRelationship",
        "partnercentral:ListRelationships",
```

```
        "partnercentral:CreateChannelHandshake",
        "partnercentral:AcceptChannelHandshake",
        "partnercentral:RejectChannelHandshake",
        "partnercentral:CancelChannelHandshake",
        "partnercentral:ListChannelHandshakes"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/program-management-account/*",
        "arn:aws:partnercentral:*:*:catalog/*/channel-handshake/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "ChannelUser"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Resell_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Partner Central und verwandte Programme AWS-Services.

`AWSPartnerCentralFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. November 2024, 23:33 UTC
- Bearbeitete Zeit: 1. Dezember 2025, 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassAWSPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "Partnercentral-account-management:AssociatePartnerUser",
        "Partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "VerificationAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartVerification",
        "partnercentral:GetVerification"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ChannelBillingTransferRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferManagement",
        "arn:aws:iam::*:role/PartnerCentralChannelBillingTransferReadOnly"
      ]
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "SupportAccess",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:AddCommunicationToCase",
        "support:ResolveCase",
        "support:AddAttachmentsToSet",
        "support:DescribeCommunications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListEntitiesAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeEntityAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralMarketingManagement

Beschreibung: Bietet den erforderlichen Zugriff für Marketingaktivitäten.

`AWSPartnerCentralMarketingManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralMarketingManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2025, 00:34 UTC
- Zeit bearbeitet: 1. Dezember 2025, 00:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralMarketingManagement`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PartnerCentralMarketingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessMarketingCentral"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" :
 "MarketingStaff"
        }
      }
    },
    {
      "Sid" : "PartnerDiscoveryAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:SearchPartnerProfiles",
        "partnercentral:GetPartnerProfile"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerProfileAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:StartProfileUpdateTask",
        "partnercentral:GetProfileUpdateTask",
        "partnercentral:CancelProfileUpdateTask",
        "partnercentral:PutProfileVisibility",
        "partnercentral:GetProfileVisibility"
      ],
      "Resource" : "arn:aws:partnercentral:*:*:catalog/*/partner/*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "PartnerCentralEphemeralWriteS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
```

```
      ],
      "Resource" : "arn:aws:s3:::aws-partner-central-marketplace-ephemeral-writeonly-
files/${aws:PrincipalAccount}/*"
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/MarketingCampaign_V1/
Dashboard/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralOpportunityManagement

Beschreibung: Bietet den erforderlichen Zugriff für Aktivitäten im Bereich Opportunity Management.

`AWSPartnerCentralOpportunityManagement`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralOpportunityManagement` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 14. November 2024, 19:09 UTC
- Bearbeitete Zeit: 1. Dezember 2025, 00:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralOpportunityManagement`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpportunityManagement",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:AcceptEngagementInvitation",
        "partnercentral:AssignOpportunity",
        "partnercentral:AssociateOpportunity",
        "partnercentral:CreateEngagement",
        "partnercentral:CreateEngagementContext",
        "partnercentral:CreateEngagementInvitation",
        "partnercentral:CreateOpportunity",
        "partnercentral:CreateResourceSnapshot",
        "partnercentral:CreateResourceSnapshotJob",
        "partnercentral:DeleteResourceSnapshotJob",
        "partnercentral:DisassociateOpportunity",
        "partnercentral:GetAwsOpportunitySummary",
        "partnercentral:GetEngagement",
        "partnercentral:GetEngagementInvitation",
        "partnercentral:GetOpportunity",
        "partnercentral:GetResourceSnapshot",
        "partnercentral:GetResourceSnapshotJob",
        "partnercentral:ListEngagementByAcceptingInvitationTasks",
        "partnercentral:ListEngagementFromOpportunityTasks",
```

```
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagementMembers",
        "partnercentral:ListEngagementResourceAssociations",
        "partnercentral:ListEngagements",
        "partnercentral:ListOpportunities",
        "partnercentral:ListOpportunityFromEngagementTasks",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "partnercentral:ListSolutions",
        "partnercentral:RejectEngagementInvitation",
        "partnercentral:StartEngagementByAcceptingInvitationTask",
        "partnercentral:StartEngagementFromOpportunityTask",
        "partnercentral:StartOpportunityFromEngagementTask",
        "partnercentral:StartResourceSnapshotJob",
        "partnercentral:StopResourceSnapshotJob",
        "partnercentral:SubmitOpportunity",
        "partnercentral:UpdateEngagementContext",
        "partnercentral:UpdateOpportunity"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "ListingAWSMarketplaceEntities",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSMarketplaceEntityAccess",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Solution/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/OfferSet/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace*/Offer/*"
      ]
    },
    {
      "Sid" : "LegacyPartnerCentralAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral-account-management:AccessLegacyPartnerCentral"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "partnercentral-account-management:LegacyPartnerCentralRole" : "AceManager"
        }
      }
    },
    {
      "Sid" : "PartnerDashboardAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetPartnerDashboard"
      ],
      "Resource" : [
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Opportunity_V1/Dashboard/
*",
        "arn:aws:partnercentral::*:catalog/AWS/ReportingData/Engagement_V1/Dashboard/*"
      ]
    },
    {
      "Sid" : "CollaborationChannelAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateCollaborationChannelRequest",
        "partnercentral:ListCollaborationChannels",
        "partnercentral:GetCollaborationChannel",
        "partnercentral:CreateCollaborationChannelMembers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PartnerResourceAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "partnercentral:ListPartners",
        "partnercentral:GetPartner"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    },
    {
      "Sid" : "TaggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:TagResource",
        "partnercentral:UntagResource",
        "partnercentral:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/*/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/*/resource-snapshot-job/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : [
            "AWS",
            "Sandbox"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralSandboxFullAccess

Beschreibung: Stellt den erforderlichen Zugriff für Entwicklertests im Sandbox-Katalog bereit.

`AWSPartnerCentralSandboxFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralSandboxFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. November 2024, 19:10 UTC
- Bearbeitete Zeit: 10. Dezember 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSandboxFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AWSPartnerCentralSandboxAccess",
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "partnercentral:Catalog" : "Sandbox"
        }
      }
    },
    {
      "Sid" : "PassAWSPartnerCentralSnapshotJobRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "resource-snapshot-job.partnercentral-
selling.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy

Beschreibung: Bietet Zugriff auf die, um eine Ressource ResourceSnapshotJob zu lesen und einen Snapshot davon im Ziel-Engagement zu erstellen.

`AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. Dezember 2024, 18:21 UTC
- Bearbeitungszeit: 10. Dezember 2024, 18:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerCentralSellingResourceSnapshotJobExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:CreateResourceSnapshot"
```

```
      ],
      "Resource" : [
        "arn:aws:partnercentral:*::catalog/AWS/engagement/*",
        "arn:aws:partnercentral:*::catalog/Sandbox/engagement/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "partnercentral:GetOpportunity"
      ],
      "Resource" : [
        "arn:aws:partnercentral:*:*:catalog/AWS/opportunity/*",
        "arn:aws:partnercentral:*:*:catalog/Sandbox/opportunity/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPartnerLedSupportReadOnlyAccess

Beschreibung: Diese Richtlinie kann verwendet werden, um nur Lesezugriff auf APIs die Dienstmetadaten für Dienste in Ihrem zu gewähren. AWS-Konto Sie können diese Richtlinie verwenden, um Ihren Partnern im partnergeführten Support-Programm Zugriff auf die Dienste zu gewähren, die im Abschnitt mit den Berechtigungsdetails unten angegeben sind.

`AWSPartnerLedSupportReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPartnerLedSupportReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. November 2024, 20:06 UTC
- Bearbeitete Zeit: 22. November 2024, 20:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPartnerLedSupportReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
```

```
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:describeCertificateAuthority",
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
```

```
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
```

```
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupPlans",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
```

```
        "cloudformation:describePublisher",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResources",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeStacks",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listStacks",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypeVersions",
        "cloudformation:listTypes",
        "cloudfront:describeFunction",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
```

```
        "cloudfront:getPublicKeyConfig",
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetricStreams",
        "cloudwatch:listMetrics",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineState",
```

```
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getGroup",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "connect:describeContact",
        "connect:describePhoneNumber",
        "connect:describeQuickConnect",
        "connect:describeUser",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:listContactEvaluations",
        "connect:listEvaluationFormVersions",
        "connect:listEvaluationForms",
        "connect:listPhoneNumbersV2",
        "connect:listQuickConnects",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listUsers",
```

```
        "connect:listViewVersions",
        "connect:listViews",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEndpoints",
        "dms:describeEventCategories",
        "dms:describeEventSubscriptions",
        "dms:describeEvents",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationInstances",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
```

```
        "dms:describeTableStatistics",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddressTransfers",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
```

```
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdFormat",
        "ec2:describeIdentityIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInstances",
        "ec2:describeInternetGateways",
        "ec2:describeIpamPools",
        "ec2:describeIpamScopes",
        "ec2:describeIpams",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLaunchTemplates",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeLocalGateways",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
```

```
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSnapshots",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeTransitGateways",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumeStatus",
        "ec2:describeVolumes",
```

```
        "ec2:describeVolumesModifications",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
```

```
        "ec2:searchTransitGatewayRoutes",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTaskSets",
        "ecs:describeTasks",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks",
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
```

```
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServiceUpdates",
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
```

```
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
```

```
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
```

```
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataflowGraph",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMLTaskRun",
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getMapping",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
```

```
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableVersions",
        "glue:getTables",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemaVersions",
        "glue:listSchemas",
        "glue:listSessions",
        "glue:listStatements",
        "glue:querySchemaVersionMetadata",
        "guardduty:getFindings",
        "guardduty:listDetectors",
        "guardduty:listFindings",
        "guardduty:listIPSets",
        "guardduty:listThreatIntelSets",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
```

```
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getOpenIDConnectProvider",
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getSSHPublicKey",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listSSHPublicKeys",
        "iam:listServerCertificates",
        "iam:listSigningCertificates",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
```

```
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctionUrlConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listLayerVersions",
        "lambda:listLayers",
```

```
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listVersionsByFunction",
        "logs:describeExportTasks",
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeSubscriptionFilters",
        "medialive:listChannels",
        "medialive:listInputSecurityGroups",
        "medialive:listInputs",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSmsChannel",
        "mobiletargeting:listJourneys",
        "pipes:listPipes",
        "polly:describeVoices",
        "polly:listLexicons",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
```

```
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboardVersions",
        "quicksight:listDashboards",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
```

```
        "quicksight:listTemplateVersions",
        "quicksight:listTemplates",
        "quicksight:listThemeAliases",
        "quicksight:listThemeVersions",
        "quicksight:listThemes",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBClusters",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEventSubscriptions",
        "rds:describeEvents",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
```

```
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterVersions",
        "redshift:describeClusters",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEventCategories",
        "redshift:describeEventSubscriptions",
        "redshift:describeEvents",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeLoggingStatus",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeReservedNodeOfferings",
        "redshift:describeReservedNodes",
        "redshift:describeResize",
```

```
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
```

```
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
```

```
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
        "s3:getAccelerateConfiguration",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
```

```
        "s3:getStorageLensConfiguration",
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultiRegionAccessPoints",
        "s3:listMultipartUploadParts",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
```

```
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
```

```
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubContents",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImageVersions",
        "sagemaker:listImages",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listLabelingJobs",
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelCards",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineExecutions",
```

```
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listServiceQuotas",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
```

```
            "ses:getImportJob",
            "ses:getSendQuota",
            "ses:getSendStatistics",
            "ses:listConfigurationSets",
            "ses:listContactLists",
            "ses:listContacts",
            "ses:listCustomVerificationEmailTemplates",
            "ses:listDedicatedIpPools",
            "ses:listDeliverabilityTestReports",
            "ses:listDomainDeliverabilityCampaigns",
            "ses:listEmailIdentities",
            "ses:listEmailTemplates",
            "ses:listIdentities",
            "ses:listIdentityPolicies",
            "ses:listImportJobs",
            "ses:listReceiptFilters",
            "ses:listReceiptRuleSets",
            "ses:listRecommendations",
            "ses:listTagsForResource",
            "ses:listTemplates",
            "ses:listVerifiedEmailAddresses",
            "sns:checkIfPhoneNumberIsOptedOut",
            "sns:getDataProtectionPolicy",
            "sns:getEndpointAttributes",
            "sns:getPlatformApplicationAttributes",
            "sns:getSMSAttributes",
            "sns:getSMSSandboxAccountStatus",
            "sns:getSubscriptionAttributes",
            "sns:getTopicAttributes",
            "sns:listEndpointsByPlatformApplication",
            "sns:listOriginationNumbers",
            "sns:listPhoneNumbersOptedOut",
            "sns:listPlatformApplications",
            "sns:listSMSSandboxPhoneNumbers",
            "sns:listSubscriptions",
            "sns:listSubscriptionsByTopic",
            "sns:listTopics",
            "ssm-contacts:describeEngagement",
            "ssm-contacts:describePage",
            "ssm-contacts:getContact",
            "ssm-contacts:getContactChannel",
            "ssm-contacts:getContactPolicy",
            "ssm-contacts:getRotation",
            "ssm-contacts:getRotationOverride",
```

```
            "ssm-contacts:listContactChannels",
            "ssm-contacts:listContacts",
            "ssm-contacts:listEngagements",
            "ssm-contacts:listPageReceipts",
            "ssm-contacts:listPageResolutions",
            "ssm-contacts:listPagesByContact",
            "ssm-contacts:listPagesByEngagement",
            "ssm-contacts:listPreviewRotationShifts",
            "ssm-contacts:listRotationOverrides",
            "ssm-contacts:listRotationShifts",
            "ssm-contacts:listRotations",
            "ssm-incidents:getIncidentRecord",
            "ssm-incidents:getReplicationSet",
            "ssm-incidents:getResourcePolicies",
            "ssm-incidents:getResponsePlan",
            "ssm-incidents:getTimelineEvent",
            "ssm-incidents:listIncidentRecords",
            "ssm-incidents:listRelatedItems",
            "ssm-incidents:listReplicationSets",
            "ssm-incidents:listResponsePlans",
            "ssm-incidents:listTimelineEvents",
            "ssm-sap:getApplication",
            "ssm-sap:getComponent",
            "ssm-sap:getDatabase",
            "ssm-sap:getOperation",
            "ssm-sap:getResourcePermission",
            "ssm-sap:listApplications",
            "ssm-sap:listComponents",
            "ssm-sap:listDatabases",
            "ssm-sap:listOperations",
            "ssm:describeActivations",
            "ssm:describeAssociation",
            "ssm:describeAssociationExecutionTargets",
            "ssm:describeAssociationExecutions",
            "ssm:describeAutomationExecutions",
            "ssm:describeAutomationStepExecutions",
            "ssm:describeAvailablePatches",
            "ssm:describeDocument",
            "ssm:describeDocumentPermission",
            "ssm:describeEffectiveInstanceAssociations",
            "ssm:describeEffectivePatchesForPatchBaseline",
            "ssm:describeInstanceAssociationsStatus",
            "ssm:describeInstanceInformation",
            "ssm:describeInstancePatchStates",
```

```
        "ssm:describeInstancePatchStatesForPatchGroup",
        "ssm:describeInstancePatches",
        "ssm:describeInventoryDeletions",
        "ssm:describeMaintenanceWindowExecutionTaskInvocations",
        "ssm:describeMaintenanceWindowExecutionTasks",
        "ssm:describeMaintenanceWindowExecutions",
        "ssm:describeMaintenanceWindowSchedule",
        "ssm:describeMaintenanceWindowTargets",
        "ssm:describeMaintenanceWindowTasks",
        "ssm:describeMaintenanceWindows",
        "ssm:describeMaintenanceWindowsForTarget",
        "ssm:describeOpsItems",
        "ssm:describeParameters",
        "ssm:describePatchBaselines",
        "ssm:describePatchGroupState",
        "ssm:describePatchGroups",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociationVersions",
        "ssm:listAssociations",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
```

```
        "ssm:listDocumentVersions",
        "ssm:listDocuments",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
```

```
        "waf-regional:getRegexPatternSet",
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
```

```
        "waf:listSizeConstraintSets",
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
```

```
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspacesConnectionStatus"
      ],
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPCSComputeNodePolicy

Beschreibung: Erteilt AWS PCS-Rechenknoten die Erlaubnis, sich mit AWS PCS-Clustern zu verbinden.

`AWSPCSComputeNodePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPCSComputeNodePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Juni 2025, 18:07 UTC
- Bearbeitete Zeit: 23. Juni 2025, 18:07 UTC

- ARN: `arn:aws:iam::aws:policy/AWSPCSComputeNodePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "pcs:RegisterComputeNodeGroupInstance"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPCSServiceRolePolicy

Beschreibung: Erteilt PCS die Erlaubnis, Ressourcen in Ihrem Namen zu verwalten.

`AWSPCSServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. August 2024, 16:01 UTC
- Bearbeitete Zeit: 11. September 2025, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPCSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "PermissionsToCreatePCSNetworkInterfacesInSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "PermissionsToManagePCSNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToDescribePCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
```

```
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreatePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToManagePCSLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTerminatePCSManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AWSPCSManaged" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "PermissionsToPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/*/AWSPCS*",
        "arn:aws:iam::*:role/AWSPCS*",
        "arn:aws:iam::*:role/aws-pcs/*",
        "arn:aws:iam::*:role/*/aws-pcs/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToControlClusterInstanceAttributes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
        "arn:aws:resource-groups:*:*:group/*",
        "arn:aws:ec2:*:*:fleet/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Sid" : "PermissionsToProvisionClusterInstances",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSPCSManaged" : "false"
        }
      }
    },
    {
      "Sid" : "PermissionsToTagPCSResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "CreateFleet",
            "CreateNetworkInterface"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToPublishMetrics",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/PCS"
        }
      }
```

```
    },
    {
      "Sid" : "PermissionsToManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecretVersionStage",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:pcs!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "pcs",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPriceListServiceFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Preislistenservice.

`AWSPriceListServiceFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPriceListServiceFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 22. November 2017, 00:36 UTC
- Bearbeitete Zeit: 2. Juli 2024, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPriceListServiceFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSPriceListServiceFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricing:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAAuditor

Beschreibung: Bietet Auditor-Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAAuditor`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAAuditor` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:33 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAAuditor`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:CreateCertificateAuthorityAuditReport",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetCertificateAuthorityCsr",
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:GetCertificate",
```

```
        "acm-pca:GetPolicy",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAConnectorForKubernetesPolicy

Beschreibung: Erteilt grundlegende Berechtigungen für den AWS Private CA Connector für Kubernetes.

`AWSPrivateCAConnectorForKubernetesPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAConnectorForKubernetesPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 19. Mai 2025, 19:22 UTC
- Bearbeitete Zeit: 19. Mai 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAConnectorForKubernetesPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:GetCertificate",
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:20 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:20 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:*"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAPrivilegedUser

Beschreibung: Bietet privilegierten Zertifikatsbenutzern Zugriff auf die AWS Private Certificate Authority

`AWSPrivateCAPrivilegedUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAPrivilegedUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:26 UTC
- Bearbeitete Zeit: 22. Januar 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAPrivilegedUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/*CACertificate*/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:30 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "acm-pca:DescribeCertificateAuthority",
      "acm-pca:DescribeCertificateAuthorityAuditReport",
      "acm-pca:ListCertificateAuthorities",
      "acm-pca:GetCertificateAuthorityCsr",
      "acm-pca:GetCertificateAuthorityCertificate",
      "acm-pca:GetCertificate",
      "acm-pca:GetPolicy",
      "acm-pca:ListPermissions",
      "acm-pca:ListTags"
    ],
    "Resource" : "*"
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateCAUser

Beschreibung: Ermöglicht Zertifikatsbenutzern Zugriff auf die AWS private Zertifizierungsstelle

`AWSPrivateCAUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateCAUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Februar 2023, 18:16 UTC
- Bearbeitete Zeit: 22. Januar 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateCAUser`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
```

```
    {
      "Effect" : "Deny",
      "Action" : [
        "acm-pca:IssueCertificate"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*",
      "Condition" : {
        "ArnNotLike" : {
          "acm-pca:TemplateArn" : [
            "arn:aws:acm-pca:*:*:template/EndEntityCertificate/V*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:RevokeCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:ListPermissions"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:certificate-authority/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:ListCertificateAuthorities"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateMarketplaceAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf alle administrativen Aktionen für einen AWS privaten Marketplace.

`AWSPrivateMarketplaceAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateMarketplaceAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 16:32 UTC
- Bearbeitete Zeit: 11. Juni 2025, 16:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceGetRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/*AWSServiceRoleForPrivateMarketplaceAdmin"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/private-
marketplace.marketplace.amazonaws.com/AWSServiceRoleForPrivateMarketplaceAdmin"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "private-marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceManageDelegatedAdministratorPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceEnableServiceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "organizations:ServicePrincipal" : "private-
marketplace.marketplace.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceRequestPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:AssociateProductsWithPrivateMarketplace",
        "aws-marketplace:DisassociateProductsFromPrivateMarketplace",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogAPIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:DescribeEntity",
        "aws-marketplace:StartChangeSet",
        "aws-marketplace:ListChangeSets",
        "aws-marketplace:DescribeChangeSet",
        "aws-marketplace:CancelChangeSet"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceCatalogTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : "arn:aws:aws-marketplace:*:*:AWSMarketplace/*"
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateMarketplaceRequests

Beschreibung: Ermöglicht den Zugriff auf die Erstellung von Anfragen auf einem AWS privaten Marketplace.

`AWSPrivateMarketplaceRequests`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPrivateMarketplaceRequests` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. Oktober 2019, 21:44 Uhr UTC
- Zeit bearbeitet: 19. November 2025, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPrivateMarketplaceRequests`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LegacyPrivateMarketplaceRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreatePrivateMarketplaceRequests",
        "aws-marketplace:ListPrivateMarketplaceRequests",
        "aws-marketplace:DescribePrivateMarketplaceRequests"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceManageRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
```

```
            "CreateProductProcurementRequest",
            "CancelProductProcurementRequest"
          ]
        }
      }
    },
    {
      "Sid" : "PrivateMarketplaceReadRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceListRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceReadChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceTaggingRequestsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:TagResource",
        "aws-marketplace:UntagResource",
        "aws-marketplace:ListTagsForResource"
      ],
      "Resource" : [
```

```
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProductProcurementRequest/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPrivateNetworksServiceRolePolicy

Beschreibung: Ermöglicht AWS Private Networks Service, Ressourcen im Namen des Kunden zu verwalten.

`AWSPrivateNetworksServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Dezember 2021, 23:17 Uhr UTC
- Bearbeitete Zeit: 16. Dezember 2021, 23:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSPrivateNetworksServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Private5G"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonCodeBuildProvisioningBasicAccess

Beschreibung: Permissions CodeBuild benötigt, um einen Build für AWS Proton CodeBuild Provisioning auszuführen.

`AWSProtonCodeBuildProvisioningBasicAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSProtonCodeBuildProvisioningBasicAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. November 2022, 21:04 UTC
- Zeit bearbeitet: 9. November 2022, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "proton:NotifyResourceDeploymentStatusChange",
      "Resource" : "arn:aws:proton:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonCodeBuildProvisioningServiceRolePolicy

Beschreibung: Ermöglicht AWS Proton, die Bereitstellung von Proton-Ressourcen mithilfe CodeBuild und anderer AWS Dienste in Ihrem Namen zu verwalten.

`AWSProtonCodeBuildProvisioningServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2022, 21:32 UTC
- Bearbeitete Zeit: 17. Mai 2023, 16:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonCodeBuildProvisioningServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/AWSProton*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonDeveloperAccess

Beschreibung: Ermöglicht den Zugriff auf AWS Proton APIs und die Management Console, ermöglicht jedoch keine Verwaltung von Proton-Vorlagen oder -Umgebungen.

`AWSProtonDeveloperAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSProtonDeveloperAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 17. Februar 2021, 19:02 UTC
- Bearbeitungszeit: 6. Juni 2024, 18:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonDeveloperAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
```

```
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : "codestar-connections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : "codeconnections:PassConnection",
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Proton APIs und Management Console. Zusätzlich zu diesen Berechtigungen ist Zugriff auf Amazon S3 erforderlich, um Vorlagenpakete aus Ihren S3-

Buckets zu registrieren, sowie Zugriff auf Amazon IAM, um die Servicerollen für Proton zu erstellen und zu verwalten.

`AWSProtonFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSProtonFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 19:07 UTC
- Bearbeitungszeit: 6. Juni 2024, 18:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonPermissions",
      "Effect" : "Allow",
      "Action" : [
        "proton:*",
        "codestar-connections:ListConnections",
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CreateGrantPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeStarConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:PassConnection"
```

```
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codestar-connections:PassedToService" : "proton.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CodeConnectionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:PassConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "codeconnections:PassedToService" : "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Proton APIs und Management Console.

`AWSProtonReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSProtonReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. Februar 2021, 19:09 UTC
- Zeit bearbeitet: 18. November 2022, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSProtonReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
```

```
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonServiceGitSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Proton ermöglicht, Ihre Service-, Umgebungs- und Komponentendefinitionen aus Ihrem Git-Repository mit AWS Proton zu synchronisieren.

`AWSProtonServiceGitSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. April 2023, 15:55 UTC
- Bearbeitete Zeit: 4. April 2023, 15:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonServiceGitSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProtonServiceSync",
      "Effect" : "Allow",
      "Action" : [
        "proton:GetService",
        "proton:UpdateService",
        "proton:UpdateServicePipeline",
        "proton:GetServiceInstance",
        "proton:CreateServiceInstance",
        "proton:UpdateServiceInstance",
        "proton:ListServiceInstances",
        "proton:GetComponent",
        "proton:CreateComponent",
        "proton:ListComponents",
        "proton:UpdateComponent",
        "proton:GetEnvironment",
        "proton:CreateEnvironment",
        "proton:ListEnvironments",
        "proton:UpdateEnvironment"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSProtonSyncServiceRolePolicy

Beschreibung: Richtlinie, die es AWS Proton ermöglicht, den Inhalt Ihres Git-Repositorys mit Proton zu synchronisieren oder Proton-Inhalte mit Ihren Git-Repositorys zu synchronisieren.

`AWSProtonSyncServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. November 2021, 21:14 UTC
- Bearbeitete Zeit: 5. Mai 2024, 01:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSProtonSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SyncToProton",
      "Effect" : "Allow",
```

```
      "Action" : [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessGitRepos",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSPurchaseOrdersServiceRolePolicy

Beschreibung: Erteilt Berechtigungen zum Anzeigen und Ändern von Bestellungen in der Abrechnungskonsole

`AWSPurchaseOrdersServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSPurchaseOrdersServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Mai 2020, 18:15 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSPurchaseOrdersServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetContactInformation",
        "aws-portal:*Billing",
```

```
        "consolidatedbilling:GetAccountBillingRole",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceUnits",
        "payments:GetPaymentInstrument",
        "payments:ListPaymentPreferences",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "tax:ListTaxRegistrations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupCFGCPacksPermissionsBoundary

Beschreibung: Die AWSQuick CFGCPacks PermissionsBoundary Setup-Richtlinie definiert die Liste der Berechtigungen, die in einer von Quick Setup erstellten IAM-Rolle zulässig sind. Quick Setup verwendet eine mit dieser Richtlinie erstellte Rolle, um AWS Config Conformance Packs bereitzustellen.

`AWSQuickSetupCFGCPacksPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupCFGCPacksPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:52 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ]
    },
    {
      "Sid" : "ConfigurationRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-CFGCPacks*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PutCPackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack"
      ],
      "Resource" : [
        "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "DescribeCPacksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConformancePacksSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SystemsManagerSLRCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EnableExplorerReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceSettingsForExplorerUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupDeploymentRolePolicy

Beschreibung: Stellt Berechtigungen für AWS Systems Manager Quick Setup zur Bereitstellung mehrerer Konfigurationstypen bereit. Diese Konfigurationstypen erstellen IAM-Rollen und -Automatisierungen, die wiederum häufig verwendete Amazon-Web-Services-Services und -Funktionen mit empfohlenen bewährten Methoden konfigurieren.

`AWSQuickSetupDeploymentRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupDeploymentRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 26. Juni 2024, 09:55 UTC
- Bearbeitete Zeit: 17. Dezember 2025, 15:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDeploymentRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CPacksRead",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConformancePacks",
        "config:DescribeConformancePackStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OpsPacksManage",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConformancePack",
        "config:DeleteConformancePack"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:config:*:*:conformance-pack/AWS-QuickSetup-*"
    },
    {
```

```
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPackInstance-*"
      ]
    },
    {
      "Sid" : "QSDocsRead",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSConformancePacks-*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
```

```
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSOperationsPack*",
        "arn:aws:ssm:*::document/AWSEC2-UpdateLaunchAgent",
        "arn:aws:ssm:*::document/AWS-ConfigureAWSPackage",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-RunPatchBaselineAssociation",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableConfigRecording",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*::document/AmazonCloudWatch-ManageAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-InstallAndManageCloudWatchAgent",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ConfigureDevOpsGuru",
        "arn:aws:ssm:*::document/AWSQuickSetupType-DeployConformancePack",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
```

```
    {
      "Sid" : "EventRulesManage",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/*QuickSetup-*"
      ]
    },
    {
      "Sid" : "CPacksSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
AWSServiceRoleForConfigConforms"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config-conforms.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "QSConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags",
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRolePass",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com",
```

```
            "events.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "QSConfigRoleBounded",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : [
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGCPacksPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupCFGRecordingPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary",
            "arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    },
    {
      "Sid" : "QSConfigRoleManagedPolicies",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
```

```
            "arn:aws:iam::aws:policy/
AWSSystemsManagerEnableConfigRecordingExecutionPolicy",
            "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy",
            "arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/AWSOperationsPack-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupDevOpsGuruPermissionsBoundary

Beschreibung: Die AWSQuick SetupDevOpsGuruPermissionsBoundary Richtlinie definiert die Liste der Berechtigungen, die in einer von Quick Setup erstellten IAM-Rolle zulässig sind. Quick Setup verwendet eine mit dieser Richtlinie erstellte Rolle, um Amazon DevOps Guru zu aktivieren und zu konfigurieren. Diese Richtlinie bietet auch Berechtigungen zum Aktivieren von Systems Manager Explorer.

`AWSQuickSetupDevOpsGuruPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupDevOpsGuruPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:44 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:44 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDevOpsGuruPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "CreateDevOpsGuruSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/devops-guru.amazonaws.com/
AWSServiceRoleForDevOpsGuru"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "devops-guru.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudformationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruNotificationChannelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:AddNotificationChannel"
      ],
      "Resource" : [
        "arn:aws:sns:*:*:DevOpsGuru-Default-Topic",
        "arn:aws:devops-guru:*:*:/channels"
      ]
    },
    {
      "Sid" : "DevOpsGuruConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "devops-guru:UpdateResourceCollection",
        "devops-guru:UpdateServiceIntegration"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SNSReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DevOpsGuruDefaultSNSTopicConfigurationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns:Publish",
        "sns:SetTopicAttributes",
        "sns:RemovePermission"
      ],
      "Resource" : "arn:aws:sns:*:*:DevOpsGuru-Default-Topic"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupDistributorPermissionsBoundary

Beschreibung: QuickSetup erstellt IAM-Rollen, die es ihm ermöglichen, die Systems Manager Distributor-Funktion in Ihrem Namen zu konfigurieren, und verwendet diese Richtlinie bei der Erstellung solcher Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AWSQuickSetupDistributorPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupDistributorPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:50 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:50 UTC

- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupDistributorPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DistributorAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ]
    },
    {
      "Sid" : "DistributorAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-RoleForDistributor-
*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-Distributor-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-ConfigureAWSPackage*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupEnableAREXExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die es Systems Manager ermöglichen, das AWSQuickSetupType-EnableAREX Automation-Runbook auszuführen, wodurch AWS Resource Explorer für die Verwendung mit Systems Manager aktiviert wird.

`AWSQuickSetupEnableAREXExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupEnableAREXExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 22:45 UTC
- Bearbeitete Zeit: 15. November 2024, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableAREXExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadActions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListViews"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowUpdateExistingIndexAndAssociateDefaultView",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:AssociateDefaultView"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreateViewAndIndex",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:TagResource"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*:*:view/all-resources/*",
        "arn:aws:resource-explorer-2:*:*:index/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/Type" : "QuickSetup",
          "aws:ResourceTag/Type" : "QuickSetup"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "Type"
        }
      }
    },
```

```
    {
      "Sid" : "AllowCreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupEnableDHMCExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die es Prinzipalen ermöglichen, das AWSQuickSetupType-EnableDHMC Automation-Runbook auszuführen, wodurch die Standard-Hostverwaltungskonfiguration aktiviert wird.

`AWSQuickSetupEnableDHMCExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupEnableDHMCExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 21:27 UTC
- Bearbeitete Zeit: 15. November 2024, 21:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupEnableDHMCExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-DefaultEC2MgmtRole-*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AmazonSSMManagedEC2InstanceDefaultPolicy"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetServiceSetting",
        "ssm:UpdateServiceSetting"
      ],
      "Resource" : "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-ec2-
instance-management-role"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupJITNADeploymentRolePolicy

Beschreibung: Mit dieser Richtlinie kann Quick Setup den Konfigurationstyp bereitstellen, der für die Einrichtung des just-in-time Knotenzugriffs erforderlich ist.

`AWSQuickSetupJITNADeploymentRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupJITNADeploymentRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. April 2025, 09:07 UTC
- Bearbeitete Zeit: 17. April 2025, 09:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupJITNADeploymentRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
        "arn:aws:ssm:*::document/AWSQuickSetupType-
PropagateJustInTimeNodeAccessPolicies",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
```

```
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "cloudformation.amazonaws.com"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::*:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-EnableJITNA-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-JITNA"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-SetupJITNAResources",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupManagedInstanceProfileExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen, die es Systems Manager ermöglichen, ein Standard-IAM-Instance-Profil für die Quick Setup-Funktion zu erstellen und es an EC2 Amazon-Instances anzuhängen, denen noch kein Instance-Profil angehängt ist.

`AWSQuickSetupManagedInstanceProfileExecutionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupManagedInstanceProfileExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 21:51 UTC
- Zeit bearbeitet: 5. November 2025, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManagedInstanceProfileExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:ListInstanceProfilesForRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : "iam:AddRoleToInstanceProfile",
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
```

```
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachAmazonSSMManagedInstanceCore",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess",
            "arn:aws:iam::aws:policy/AmazonElasticFileSystemsUtils",
            "arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy"
          ]
```

```
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "InstanceProfileAssociationEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutomationsStartWithTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ],
          "aws:ResourceTag/InvokedBy" : [
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "AutomationsGetPermissions",
      "Effect" : "Allow",
      "Action" : "ssm:GetAutomationExecution",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/InvokedBy" : [
```

```
            "AWSQuickSetupType-ManageInstanceProfile"
          ]
        }
      }
    },
    {
      "Sid" : "GetQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
          ]
        }
      }
    },
    {
      "Sid" : "PassQuickSetupAutomationAssumeRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM",
            "AWSQuickSetupType-SSMHostMgmt",
            "AWSQuickSetupType-PatchPolicy",
            "AWSQuickSetupType-Distributor",
            "AWSQuickSetupType-CWASetup"
```

```
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupManageJITNAResourcesExecutionPolicy

Beschreibung: Diese Richtlinie bietet Berechtigungen zum Aktivieren des just-in-time Knotenzugriffs für Systems Manager.

`AWSQuickSetupManageJITNAResourcesExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupManageJITNAResourcesExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. April 2025, 21:37 UTC
- Bearbeitete Zeit: 23. April 2025, 15:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupManageJITNAResourcesExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateJustInTimeAccessServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/justintimeaccess.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerJustInTimeAccess"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "justintimeaccess.ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateSystemsManagerNotificationServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/notifications.ssm.amazonaws.com/
AWSServiceRoleForSystemsManagerNotifications"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "notifications.ssm.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::*:policy/
AWSSystemsManagerJustInTimeAccessTokenPolicy"
        }
      }
    },
    {
      "Sid" : "IAMRoleManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SSM-JustInTimeAccessTokenRole"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-JITNA"
          ]
        }
      }
    },
    {
      "Sid" : "ServiceSettingsManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/just-in-time-access/identity-provider"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupPatchPolicyBaselineAccess

Beschreibung: Stellt schreibgeschützte Berechtigungen für den Zugriff auf Patch-Baselines bereit, die von einem Administrator in der aktuellen AWS-Konto oder der Organisation mithilfe von Quick Setup konfiguriert wurden.

`AWSQuickSetupPatchPolicyBaselineAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupPatchPolicyBaselineAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:38 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3SameAccountReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalAccount" : [
            "${aws:ResourceAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "QuickSetupPatchingBaselineOverridesS3OrganizationReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalOrgID" : [
            "${aws:ResourceOrgID}"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupPatchPolicyDeploymentRolePolicy

Beschreibung: Stellt Berechtigungen bereit, die es Quick Setup ermöglichen, Ressourcen zu erstellen, die einer Patch-Richtlinienkonfiguration zugeordnet sind.

`AWSQuickSetupPatchPolicyDeploymentRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupPatchPolicyDeploymentRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:57 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:57 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyDeploymentRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnRead",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "RGroupsGet",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "S3BucketsList",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AccessLogsBucketManage",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:Put*",
        "s3:Get*",
        "s3:List*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:s3:::aws-quicksetup-patchpolicy-access-log-*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:UpdateFunction*",
```

```
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:DeleteFunction",
        "lambda:InvokeFunction",
        "lambda:UntagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ]
    },
    {
      "Sid" : "LogGroupsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogGroupsManage",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource",
        "logs:PutRetentionPolicy",
        "logs:DeleteLogGroup",
        "logs:ListTagsForResource",
        "logs:UntagResource"
      ],
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "QSDocsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument",
        "ssm:UpdateDocument",
        "ssm:DescribeDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:ListTagsForResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*"
      ]
    },
    {
      "Sid" : "QSDocsGet",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
```

```
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline"
      ]
    },
    {
      "Sid" : "QSAssociationsManage",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-RunPatchBaseline",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "ConfigRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole",
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid" : "ConfigRolePassToSSM",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "ConfigRolePassToLambda",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DocDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LegacyDocClean",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "LegacyIAMClean",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
```

```
        "iam:DeleteRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/*QuickSetup-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/QuickSetupID" : "*"
        }
      }
    },
    {
      "Sid" : "ConfigRoleBoundedManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:PutRolePermissionsBoundary"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
AWSQuickSetupPatchPolicyPermissionsBoundary"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupPatchPolicyPermissionsBoundary

Beschreibung: QuickSetup erstellt IAM-Rollen, die es ihm ermöglichen, die Systems Manager Patch Manager-Funktion in Ihrem Namen zu konfigurieren, und verwendet diese Richtlinie bei der Erstellung solcher Rollen, um die Grenzen ihrer Berechtigungen zu definieren.

`AWSQuickSetupPatchPolicyPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupPatchPolicyPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:46 UTC
- Bearbeitete Zeit: 12. September 2025, 15:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "PatchingAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ]
    },
    {
      "Sid" : "PatchingAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
```

```
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AWSQuickSetupPatchPolicyBaselineAccess"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-AutomationRole-*"
        }
      },
      "Resource" : "arn:aws:iam::*:role/*"
```

```
    },
    {
      "Sid" : "CreateSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "InstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ManagedInstanceRoleUpdatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateManagedInstanceRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "InstanceProfileCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "InstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "InstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
```

```
    },
    {
      "Sid" : "SSMAssociationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:UpdateAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "BaselineS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:Put*",
        "s3:Get*",
        "s3:List*",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteBucket"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      },
      "Resource" : "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    },
    {
      "Sid" : "PatchingFunctionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
```

```
        "arn:aws:lambda:*:*:function:baseline-overrides-*",
        "arn:aws:lambda:*:*:function:delete-name-tags-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    },
    {
      "Sid" : "LoggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/baseline-overrides-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/delete-name-tags-*"
      ]
    },
    {
      "Sid" : "SSMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:managed-instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "EC2TaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigName-*"
        }
      }
    },
    {
      "Sid" : "RoleTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QSConfigId-*"
        }
      }
    },
    {
      "Sid" : "PatchingReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetPatchBaseline",
        "ssm:GetInventory",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAssociation",
        "ssm:GetAutomationExecution",
        "ssm:ListTagsForResource",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PatchingAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer*",
```

```
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/QuickSetup-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:document/AWS-EnableExplorer*",
        "arn:aws:ssm:*:*:document/AWS-RunPatchBaseline*",
        "arn:aws:ssm:*:*:document/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:document/QuickSetup-*",
        "arn:aws:ssm:*:*:document/AWSQuickSetup-*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSchedulerPermissionsBoundary

Beschreibung: Die AWSQuick SetupSchedulerPermissionsBoundary Richtlinie definiert die Liste der Berechtigungen, die in einer von Quick Setup erstellten IAM-Rolle zulässig sind. Quick Setup verwendet eine mit dieser Richtlinie erstellte Rolle, um geplante Operationen auf EC2 Amazon-Instances und anderen Ressourcen zu aktivieren und zu konfigurieren.

`AWSQuickSetupSchedulerPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSchedulerPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:53 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSchedulerPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ConfigurationAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ]
    },
    {
      "Sid" : "ConfigurationAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-Scheduler-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SystemsManagerCalendarReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar-*"
```

```
      ]
    },
    {
      "Sid" : "EC2ReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2StartStopPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AutomationStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
StartStateManagerAssociations-*"
      ]
    },
    {
      "Sid" : "AssociationsStartOncePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSSMDeploymentRolePolicy

Beschreibung: Diese Richtlinie gewährt Administratorrechte, die es Quick Setup ermöglichen, Ressourcen zu erstellen, die während des Systems Manager Manager-Onboarding-Prozesses verwendet werden.

`AWSQuickSetupSSMDeploymentRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSSMDeploymentRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 22:53 UTC
- Bearbeitete Zeit: 27. Oktober 2025, 11:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DetectStackDrift",
        "cloudformation:DetectStackResourceDrift",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-SSM-*"
      ]
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:TagResource"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunction*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ],
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation",
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
```

```
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
        "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
        "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
        "arn:aws:ssm:*::document/AWS-EnableExplorer",
        "arn:aws:ssm:*::document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*::document/AWS-UpdateSSMAgent",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Sid" : "SSMSLRCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:TagRole"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
```

```
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "QuickSetup*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ],
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateRole",
        "iam:DeleteRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/
AWSQuickSetupSSMLifecycleManagementExecutionPolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupSSMManageResourcesExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
AdministrationRolePolicy",
```

```
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
ExecutionRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-RemediationAutomation-
OperationalAccountAdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-Automation-DiagnosisBucketPolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-
AdministrationRolePolicy",
            "arn:aws:iam::aws:policy/AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy"
          ]
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableAREX",
            "arn:aws:ssm:*::document/AWSQuickSetupType-EnableDHMC",
            "arn:aws:ssm:*::document/AWSQuickSetupType-ManageInstanceProfile",
            "arn:aws:ssm:*::document/AWS-EnableExplorer",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
```

```
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-LifecycleManagement*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com",
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:TagResource",
      "Resource" : [
        "arn:aws:lambda:*:*:function:aws-quicksetup-lifecycle*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-*",
```

```
        "arn:aws:iam::*:role/AWS-SSM-Remediation*",
        "arn:aws:iam::*:role/AWS-SSM-Diagnosis*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "QuickSetup*"
        },
        "StringLike" : {
          "aws:RequestTag/QuickSetupDocumentVersionName" : "*"
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : "arn:aws:ssm:*::document/AWSQuickSetupType-SSM-ManageResources"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeAssociationExecutions",
        "ssm:DescribeAssociationExecutionTargets",
        "ssm:GetAutomationExecution"
      ],
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "cloudformation.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      },
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:association/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSSMDeploymentS3BucketRolePolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Auflisten aller S3-Buckets in einem Konto sowie zum Verwalten und Abrufen von Informationen zu bestimmten Buckets im Hauptkonto, die über Vorlagen verwaltet werden. AWS CloudFormation

`AWSQuickSetupSSMDeploymentS3BucketRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSSMDeploymentS3BucketRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 22:01 UTC
- Bearbeitete Zeit: 15. November 2024, 22:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentS3BucketRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketTagging",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSSMHostMgmtPermissionsBoundary

Beschreibung: Quick Setup erstellt IAM-Rollen, die es ermöglichen, den Host Manager Quick Setup-Typ in Ihrem Namen zu konfigurieren, und verwendet diese Richtlinie, wenn solche Rollen erstellt werden, um die Grenzen ihrer Berechtigungen zu definieren.

`AWSQuickSetupSSMHostMgmtPermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSSMHostMgmtPermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:48 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:48 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMHostMgmtPermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HostManagementAutomationRoleGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ]
    },
    {
      "Sid" : "HostManagementAutomationRolePassPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleManagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:UpdateRole",
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRolePassToSSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonSSMRoleForInstancesQuickSetup"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "InstanceManagementPoliciesAttachPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore",
            "arn:aws:iam::aws:policy/AmazonSSMPatchAssociation"
          ]
        },
        "StringLike" : {
          "aws:PrincipalTag/QuickSetupManagerID" : "*"
        },
        "ArnLike" : {
          "aws:PrincipalArn" : "arn:aws:iam::*:role/AWS-QuickSetup-HostMgmtRole-*"
        }
```

```
      },
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceRoleAddPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileCreatePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AmazonSSMRoleForInstancesQuickSetup"
      ]
    },
    {
      "Sid" : "DefaultInstanceProfileAssociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:InstanceProfile" : "true"
        },
        "ArnLike" : {
          "ec2:NewInstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "DefaultInstanceProfileDisassociationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/
AmazonSSMRoleForInstancesQuickSetup"
        }
      }
    },
    {
      "Sid" : "ConfigurationAutomationsStartPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-HostMgmt-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
CreateAndAttachIAMToInstance-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
UpdateExistingInstanceProfile-*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetup-
InstallAndManageCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/UpdateCloudWatchDocument-*",
        "arn:aws:ssm:*:*:automation-definition/AWSEC2-UpdateLaunchAgent-*",
        "arn:aws:ssm:*:*:automation-definition/AWS-AttachIAMToInstance*",
        "arn:aws:ssm:*:*:automation-definition/AWS-GatherSoftwareInventory*",
        "arn:aws:ssm:*:*:automation-definition/AWS-RunPatchBaselineAssociation*",
        "arn:aws:ssm:*:*:automation-definition/AWS-UpdateSSMAgent*"
      ]
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingHostManagementBySSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource",
        "ssm:GetAutomationExecution",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
```

```
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSSMLifecycleManagementExecutionPolicy

Beschreibung: Die Richtlinie gewährt Administratorberechtigungen, die es Quick Setup ermöglichen, während der Quick Setup-Bereitstellung in Systems Manager eine AWS CloudFormation benutzerdefinierte Ressource für Lebenszyklusereignisse auszuführen.

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSSMLifecycleManagementExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 21:55 UTC
- Bearbeitete Zeit: 12. September 2025, 15:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMLifecycleManagementExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetAutomationExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageResources*",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ],
          "iam:ResourceTag/QuickSetupDocument" : [
            "AWSQuickSetupType-SSM"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution",
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-SSM-ManageResources*",
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupSSMManageResourcesExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die es Systems Manager ermöglichen, Voraussetzungen wie IAM-Rollen zu erstellen, die für das Onboarding von Systems Manager erforderlich sind.

`AWSQuickSetupSSMManageResourcesExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupSSMManageResourcesExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2024, 22:49 UTC
- Bearbeitete Zeit: 15. November 2024, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupSSMManageResourcesExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
```

```
        "iam:TagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:ResourceTag/QuickSetupDocument" : "AWSQuickSetupType-SSM",
          "aws:RequestTag/QuickSetupDocument" : "AWSQuickSetupType-SSM"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*",
        "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy"
          ]
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableExplorer*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableDHMCExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableDHMC*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupManagedInstanceProfileExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-ManageInstanceProfile*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/
AWSQuickSetupEnableAREXExecutionPolicy"
        }
      },
      "Resource" : "arn:aws:iam::*:role/AWS-QuickSetup-SSM-EnableAREX*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:ListBucketVersions",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::do-not-delete-ssm-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : [
            "${aws:PrincipalAccount}"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupStartSSMAssociationsExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die es Prinzipalen ermöglichen, das AWSQuickSetupType-StartSSMAssociations Automation-Runbook auszuführen, wodurch State Manager Associations gestartet werden.

`AWSQuickSetupStartSSMAssociationsExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupStartSSMAssociationsExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. August 2025, 12:04 UTC
- Bearbeitete Zeit: 12. September 2025, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartSSMAssociationsExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ChangeCalendarState",
            "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ChangeCalendarState*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSetupStartStopInstancesExecutionPolicy

Beschreibung: Die verwaltete Richtlinie AWSQuick SetupStartStopInstancesExecutionPolicy gewährt Quick Setup die Erlaubnis, EC2 Amazon-Instances nach einem Zeitplan zu starten und zu beenden. Diese Richtlinie wird mit dem Konfigurationstyp Quick Setup Scheduler verwendet.

`AWSQuickSetupStartStopInstancesExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSetupStartStopInstancesExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. August 2025, 12:04 UTC
- Bearbeitete Zeit: 12. September 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSetupStartStopInstancesExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions",
        "ec2:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetCalendarState"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/AWSQuickSetup-ChangeCalendar*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
        "arn:aws:ssm:*:*:automation-execution/*",
        "arn:aws:ssm:*:*:automation-definition/AWSQuickSetupType-Scheduler-
ApplyInstanceState*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWS-QuickSetup*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceARN" : [
            "arn:aws:ssm:*::document/AWSQuickSetupType-Scheduler-ApplyInstanceState",
            "arn:aws:ssm:*:*:association/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightAssetBundleExportPolicy

Beschreibung: Stellt die Berechtigungen bereit, die für die Ausführung von QuickSight Asset Bundle-Exportvorgängen erforderlich sind

`AWSQuickSightAssetBundleExportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightAssetBundleExportPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2024, 21:31 UTC
- Bearbeitete Zeit: 27. März 2024, 21:31 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleExportPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAnalysis",
        "quicksight:DescribeAnalysisPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:ListRefreshSchedules",
        "quicksight:DescribeDataSetPermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
```

```
      "Sid" : "DataSourceReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeTheme",
        "quicksight:DescribeThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "VPCConnectionReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeVPCConnection",
        "quicksight:ListVPCConnections"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "RefreshScheduleReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "AssetBundleExportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleExportJob",
        "quicksight:ListAssetBundleExportJobs",
        "quicksight:StartAssetBundleExportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-export-job/*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightAssetBundleImportPolicy

Beschreibung: Stellt die Berechtigungen bereit, die für die Durchführung von QuickSight Asset-Bundle-Importvorgängen erforderlich sind

`AWSQuickSightAssetBundleImportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightAssetBundleImportPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. März 2024, 21:40 UTC
- Bearbeitete Zeit: 27. März 2024, 21:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightAssetBundleImportPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListTagsForResource",
        "quicksight:TagResource",
        "quicksight:UntagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:*/*"
    },
    {
      "Sid" : "DashboardWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDashboard",
        "quicksight:DeleteDashboard",
        "quicksight:DescribeDashboard",
        "quicksight:UpdateDashboard",
        "quicksight:UpdateDashboardPublishedVersion",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:UpdateDashboardPermissions",
        "quicksight:UpdateDashboardLinks"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dashboard/*"
    },
    {
      "Sid" : "AnalysisWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateAnalysis",
        "quicksight:DeleteAnalysis",
        "quicksight:DescribeAnalysis",
        "quicksight:UpdateAnalysis",
        "quicksight:DescribeAnalysisPermissions",
        "quicksight:UpdateAnalysisPermissions"
```

```
      ],
      "Resource" : "arn:aws:quicksight:*:*:analysis/*"
    },
    {
      "Sid" : "DataSetWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:DeleteDataSet",
        "quicksight:DescribeDataSet",
        "quicksight:PassDataSet",
        "quicksight:UpdateDataSet",
        "quicksight:DeleteDataSetRefreshProperties",
        "quicksight:DescribeDataSetRefreshProperties",
        "quicksight:PutDataSetRefreshProperties",
        "quicksight:UpdateDataSetPermissions",
        "quicksight:DescribeDataSetPermissions",
        "quicksight:ListRefreshSchedules"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*"
    },
    {
      "Sid" : "DataSourceWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:DescribeDataSource",
        "quicksight:DeleteDataSource",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSourcePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*"
    },
    {
      "Sid" : "ThemeWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateTheme",
        "quicksight:DeleteTheme",
        "quicksight:DescribeTheme",
        "quicksight:UpdateTheme",
        "quicksight:DescribeThemePermissions",
```

```
        "quicksight:UpdateThemePermissions"
      ],
      "Resource" : "arn:aws:quicksight:*:*:theme/*"
    },
    {
      "Sid" : "RefreshScheduleWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateRefreshSchedule",
        "quicksight:DescribeRefreshSchedule",
        "quicksight:DeleteRefreshSchedule",
        "quicksight:UpdateRefreshSchedule"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*/refresh-schedule/*"
    },
    {
      "Sid" : "VPCConnectionWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:ListVPCConnections",
        "quicksight:CreateVPCConnection",
        "quicksight:DescribeVPCConnection",
        "quicksight:DeleteVPCConnection",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : "arn:aws:quicksight:*:*:vpcConnection/*"
    },
    {
      "Sid" : "AssetBundleImportOperations",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAssetBundleImportJob",
        "quicksight:ListAssetBundleImportJobs",
        "quicksight:StartAssetBundleImportJob"
      ],
      "Resource" : "arn:aws:quicksight:*:*:asset-bundle-import-job/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuicksightAthenaAccess

Beschreibung: Quicksight-Zugriff auf die Athena-API und S3-Buckets, die für Athena-Abfrageergebnisse verwendet werden

`AWSQuicksightAthenaAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSQuicksightAthenaAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 9. Dezember 2016, 02:31 Uhr UTC
- Zeit bearbeitet: 03. Januar 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightAthenaAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGetQueryExecution",
        "athena:CancelQueryExecution",
        "athena:GetCatalogs",
        "athena:GetExecutionEngine",
        "athena:GetExecutionEngines",
        "athena:GetNamespace",
        "athena:GetNamespaces",
        "athena:GetQueryExecution",
        "athena:GetQueryExecutions",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetTable",
        "athena:GetTables",
        "athena:ListQueryExecutions",
        "athena:RunQuery",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "athena:ListWorkGroups",
        "athena:ListEngineVersions",
        "athena:GetWorkGroup",
        "athena:GetDataCatalog",
        "athena:GetDatabase",
        "athena:GetTableMetadata",
        "athena:ListDataCatalogs",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UpdateDatabase",
        "glue:CreateTable",
```

```
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:GetTables",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-athena-query-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightDescribeRDS

Beschreibung: QuickSight Erlaubt die Beschreibung der RDS-Ressourcen

`AWSQuickSightDescribeRDS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightDescribeRDS` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. November 2015, 23:24 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:24 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRDS`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "rds:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightDescribeRedshift

Beschreibung: Erlaubt QuickSight die Beschreibung von Redshift-Ressourcen

`AWSQuickSightDescribeRedshift`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightDescribeRedshift` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. November 2015, 23:25 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:25 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightDescribeRedshift`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "redshift:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightElasticsearchPolicy

Beschreibung: Bietet Zugriff auf Amazon Elasticsearch-Ressourcen von Amazon QuickSight

`AWSQuickSightElasticsearchPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightElasticsearchPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 09. September 2020, 17:27 UTC
- Bearbeitete Zeit: 7. September 2021, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightElasticsearchPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeElasticsearchDomain",
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightIoTAnalyticsAccess

Beschreibung: Geben Sie QuickSight schreibgeschützten Zugriff auf IoT Analytics Analytics-Datensätze

`AWSQuickSightIoTAnalyticsAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightIoTAnalyticsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 17:00 Uhr UTC
- Zeit bearbeitet: 29. November 2017, 17:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightIoTAnalyticsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iotanalytics:ListDatasets",
        "iotanalytics:DescribeDataset",
        "iotanalytics:GetDatasetContent"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightListIAM

Beschreibung: Erlaubt QuickSight das Auflisten von IAM-Entitäten

`AWSQuickSightListIAM`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightListIAM` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 10. November 2015, 23:25 Uhr UTC
- Zeit bearbeitet: 10. November 2015, 23:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightListIAM`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuicksightOpenSearchPolicy

Beschreibung: Bietet Zugriff auf OpenSearch Amazon-Ressourcen von Amazon QuickSight

`AWSQuicksightOpenSearchPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuicksightOpenSearchPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 7. September 2021, 23:26 UTC
- Bearbeitete Zeit: 7. September 2021, 23:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuicksightOpenSearchPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/",
        "arn:aws:es:*:*:domain/*/_cluster/settings",
        "arn:aws:es:*:*:domain/*/_cat/indices"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "es:ListDomainNames",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:DescribeDomain"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*"
```

```
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "es:ESHttpPost",
        "es:ESHttpGet"
      ],
      "Resource" : [
        "arn:aws:es:*:*:domain/*/_opendistro/_sql",
        "arn:aws:es:*:*:domain/*/_plugin/_sql"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightSageMakerPolicy

Beschreibung: Bietet Zugriff auf SageMaker Amazon-Ressourcen von Amazon QuickSight

`AWSQuickSightSageMakerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightSageMakerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 17. Januar 2020, 17:18 Uhr UTC

- Bearbeitete Zeit: 30. Oktober 2023, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSageMakerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SageMakerTransformJobAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:CreateTransformJob"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:transform-job/quicksight-auto-generated-*"
    },
    {
      "Sid" : "SageMakerModelReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListModels",
        "sagemaker:DescribeModel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ObjectReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
```

```
        "arn:aws:s3:::quicksight-ml.*",
        "arn:aws:s3:::sagemaker*"
      ]
    },
    {
      "Sid" : "S3ObjectUpdateAccess",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::sagemaker*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3BucketReadAccess",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::sagemaker*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightSecretsManagerWriteAccess

Beschreibung: Richtlinie, die verwendet wird QuickSight , um Geheimnisse in AWS Secrets Manager zu erstellen und Ressourcenrichtlinien an bestehende QuickSight Geheimnisse anzuhängen.

`AWSQuickSightSecretsManagerWriteAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightSecretsManagerWriteAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 22. Mai 2025, 01:22 UTC
- Bearbeitete Zeit: 22. Mai 2025, 01:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightSecretsManagerWriteAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightSecretsManagerWritePolicy

Beschreibung: Richtlinie, die verwendet wird QuickSight , um Geheimnisse in AWS Secrets Manager zu erstellen und Ressourcenrichtlinien an bestehende QuickSight Geheimnisse anzuhängen.

`AWSQuickSightSecretsManagerWritePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightSecretsManagerWritePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. Mai 2025, 19:22 UTC
- Bearbeitete Zeit: 12. Mai 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSQuickSightSecretsManagerWritePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "quicksight",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:quicksight!*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "secretsmanager:Name" : "quicksight!*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSQuickSightTimestreamPolicy

Beschreibung: AWS QuickSight Zugriff auf AWS Timestream APIs. Kunden können diese Richtlinie an AWS QuickSight eine Rolle anhängen, um das Abrufen von Daten und Metadaten zu ermöglichen.

`AWSQuickSightTimestreamPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSQuickSightTimestreamPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 30. September 2020, 21:47 Uhr UTC
- Bearbeitete Zeit: 30. September 2020, 21:47 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSQuickSightTimestreamPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "timestream:Select",
        "timestream:CancelQuery",
        "timestream:ListTables",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:DescribeTable",
        "timestream:DescribeDatabase",
        "timestream:SelectValues",
        "timestream:DescribeEndpoints"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSReachabilityAnalyzerServiceRolePolicy

Beschreibung: Ermöglicht VPC Reachability Analyzer den Zugriff auf AWS Ressourcen und die Integration mit AWS Organizations in Ihrem Namen.

`AWSReachabilityAnalyzerServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. November 2022, 17:12 UTC
- Bearbeitete Zeit: 10. September 2024, 16:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSReachabilityAnalyzerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReachabilityAnalyzerPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualGateways",
        "directconnect:DescribeVirtualInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
```

```
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "resource-groups:ListGroups",
        "resource-groups:ListGroupResources",
        "tag:GetResources",
        "tiros:CreateQuery",
        "tiros:ExtendQuery",
        "tiros:GetQueryAnswer",
        "tiros:GetQueryExplanation",
        "tiros:GetQueryExtensionAccounts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ApigatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRefactoringToolkitFullAccess

Beschreibung: Diese Richtlinie gewährt die Erlaubnis zur Nutzung von AWS Diensten mit der AWS Toolkit for .NET Refactoring-Erweiterung für Microsoft Visual Studio. Sie soll an ein lokales Profil angehängt werden. AWS Die Richtlinie ermöglicht das Hochladen von Anwendungsartefakten und das Herunterladen der resultierenden Artefakte von Amazon S3. Es ermöglicht das Erstellen von Anwendungen in einem Container-Image mithilfe AWS CodeBuild und Speichern und Abrufen der Images aus Amazon Elastic Container Registry (Amazon ECR). Und es ermöglicht die Bereitstellung der Anwendung für Container-Services AWS wie Amazon Elastic Container Service (Amazon ECS), die optionale Erstellung von VPC-Ressourcen, die optionale Verbindung zu vorhandener Infrastruktur wie AWS Directory Service und andere verwandte Dienste.

`AWSRefactoringToolkitFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRefactoringToolkitFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2022, 16:41 UTC
- Bearbeitete Zeit: 09. April 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a2c:GetContainerizationJobDetails",
        "a2c:GetDeploymentJobDetails",
        "a2c:StartContainerizationJob",
        "a2c:StartDeploymentJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateStack",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:*:cloudformation:*:*:stack/a2c-app-*",
        "arn:*:cloudformation:*:*:stack/a2c-build-*",
        "arn:*:cloudformation:*:*:stack/application-transformation-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:CreateProject",
        "codebuild:UpdateProject"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "codebuild:StartBuild"
      ],
      "Resource" : "arn:aws:codebuild:*:*:project/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
```

```
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "AuthorizeSecurityGroupIngress",
            "CreateInternetGateway",
            "CreateKeyPair",
            "CreateRoute",
            "CreateRouteTable",
            "CreateSubnet",
            "CreateVpc"
          ]
        },
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
```

```
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-transformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable",
        "ec2:AttachInternetGateway",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteTags",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateSubnet",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetLifecyclePolicy",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecr:TagResource",
        "ecr:UntagResource"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:CreateService",
        "ecs:RegisterTaskDefinition",
        "ecs:TagResource"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "a2c-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:ExecuteCommand"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ecs:container-name" : "application-transformation-sidecar"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/a2c-generated" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "a2c-generated"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/application-transformation" : "false"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "application-transformation"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/codebuild/*:*",
```

```
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/a2c-generated" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/ecs/containerinsights/*:*",
        "arn:aws:logs:*:*:log-group:/aws/ecs/container-logs/*:*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource",
        "ssm:GetParameters",
        "ssm:PutParameter",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/a2c-generated-check-ecs-slr-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeSessions",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:CreateDataChannel",
        "ssmmessages:OpenControlChannel",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/refactoringtoolkit*",
        "arn:aws:s3:::*/a2c-generated*",
        "arn:aws:s3:::*/application-transformation*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "application-transformation",
            "refactoringtoolkit"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "clouddirectory:ListDirectories",
        "codebuild:BatchGetProjects",
        "codebuild:BatchGetBuilds",
        "ds:DescribeDirectories",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "ecr:DescribeImages",
        "ecr:DescribeRepositories",
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ecs:DescribeTasks",
        "ecs:ListTagsForResource",
        "ecs:ListTasks",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListAllMyBuckets",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore",
        "arn:aws:s3:::aws.portingassistant.dotnet.datastore/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "application-transformation:StartPortingCompatibilityAssessment",
        "application-transformation:GetPortingCompatibilityAssessment",
        "application-transformation:StartPortingRecommendationAssessment",
        "application-transformation:GetPortingRecommendationAssessment",
        "application-transformation:PutLogData",
```

```
        "application-transformation:PutMetricData",
        "application-transformation:StartContainerization",
        "application-transformation:GetContainerization",
        "application-transformation:StartDeployment",
        "application-transformation:GetDeployment"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:*:ecr:*:*:repository/*",
      "Condition" : {
        "Null" : {
          "ecr:ResourceTag/application-transformation" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*::*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "ForAnyValue:StringLike" : {
          "kms:ResourceAliases" : "alias/application-transformation*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRefactoringToolkitSidecarPolicy

Beschreibung: Diese Richtlinie ist für Amazon ECS-Aufgaben vorgesehen, die zum Testen von Anwendungen AWS mithilfe der AWS Toolkit for .NET Refactoring-Erweiterung für Microsoft Visual Studio erstellt wurden. Die Richtlinie gewährt Zugriff auf das Herunterladen von Anwendungsartefakten von Amazon S3, die Übermittlung des Status der Aufgabe mithilfe von AWS Systems Manager und andere erforderliche Dienste.

`AWSRefactoringToolkitSidecarPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRefactoringToolkitSidecarPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2022, 16:41 UTC
- Bearbeitete Zeit: 29. Oktober 2022, 22:15 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRefactoringToolkitSidecarPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmMessagesAccess",
      "Effect" : "Allow",
      "Action" : [
        "ssmmessages:OpenControlChannel",
        "ssmmessages:CreateControlChannel",
        "ssmmessages:OpenDataChannel",
        "ssmmessages:CreateDataChannel"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3GetObjectAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::*/refactoringtoolkit*"
    },
    {
      "Sid" : "S3ListBucketAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : "refactoringtoolkit*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSrePostPrivateCloudWatchAccess

Beschreibung: Bietet re:POST Private-Zugriff zum Veröffentlichen CloudWatch von Metrikdaten

`AWSrePostPrivateCloudWatchAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2023, 16:37 UTC
- Bearbeitete Zeit: 15. November 2023, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSrePostPrivateCloudWatchAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchPublishMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/rePostPrivate",
            "AWS/Usage"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRepostSpaceSupportOperationsPolicy

Beschreibung: Diese Richtlinie ermöglicht es dem re:POST Space-Dienst, Supportanfragen zu erstellen, zu verwalten und zu lösen, die über die Space-Anwendung erstellt wurden.

`AWSRepostSpaceSupportOperationsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRepostSpaceSupportOperationsPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2023, 21:52 UTC
- Bearbeitete Zeit: 26. November 2023, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRepostSpaceSupportOperationsPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RepostSpaceSupportOperations",
      "Effect" : "Allow",
      "Action" : [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResilienceHubAsssessmentExecutionPolicy

Beschreibung: Richtlinie für die AWS Resilience Hub-Dienstrolle, die den Zugriff auf andere AWS Dienste ermöglicht, um die Bewertung durchzuführen.

`AWSResilienceHubAsssessmentExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResilienceHubAsssessmentExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2023, 12:32 UTC
- Bearbeitete Zeit: 16. Dezember 2024, 14:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSResilienceHubFullResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "autoscaling:DescribeAutoScalingGroups",
        "backup:DescribeBackupVault",
        "backup:GetBackupPlan",
        "backup:GetBackupSelection",
        "backup:ListBackupPlans",
        "backup:ListBackupSelections",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ValidateTemplate",
```

```
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "datasync:DescribeTask",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "devops-guru:ListMonitoredResources",
        "dlm:GetLifecyclePolicies",
        "dlm:GetLifecyclePolicy",
        "docdb-elastic:GetCluster",
        "docdb-elastic:GetClusterSnapshot",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobs",
        "drs:DescribeSourceServers",
        "drs:GetReplicationConfiguration",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeFastSnapshotRestores",
        "ec2:DescribeFleets",
        "ec2:DescribeHosts",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRegions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcEndpoints",
        "ecr:DescribeRegistry",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
```

```
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeServerlessCaches",
        "elasticache:DescribeServerlessCacheSnapshots",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "fis:GetExperiment",
        "fis:GetExperimentTemplate",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListExperimentResolvedTargets",
        "fsx:DescribeFileSystems",
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctionEventInvokeConfigs",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBSnapshots",
        "rds:DescribeGlobalClusters",
        "rds:ListTagsForResource",
        "resource-groups:GetGroup",
        "resource-groups:ListGroupResources",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
```

```
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-readiness:GetReadinessCheckStatus",
        "route53-recovery-readiness:GetResourceSet",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:ListBucket",
        "servicecatalog:GetApplication",
        "servicecatalog:ListAssociatedResources",
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "ssm:DescribeAutomationExecutions",
        "states:DescribeStateMachine",
        "states:ListStateMachineVersions",
        "states:ListStateMachineAliases",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSResilienceHubApiGatewayStatement",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/usageplans"
      ]
    },
    {
      "Sid" : "AWSResilienceHubS3ArtifactStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutObject",
```

```
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::aws-resilience-hub-artifacts-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubS3AccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
        "s3:GetBucketVersioning",
        "s3:GetMultiRegionAccessPointRoutes",
        "s3:GetReplicationConfiguration",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AWSResilienceHubCloudWatchStatement",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "ResilienceHub"
        }
      }
    },
```

```
    {
      "Sid" : "AWSResilienceHubSSMStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Resource Access Manager

`AWSResourceAccessManagerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceAccessManagerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2019, 17:28 UTC
- Bearbeitete Zeit: 4. Juni 2019, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Resource Access Manager.

`AWSResourceAccessManagerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceAccessManagerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Dezember 2019, 20:58 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerResourceShareParticipantAccess

Beschreibung: Ermöglicht den Zugriff auf AWS Resource Access Manager, den ein Resource Share-Teilnehmer APIs benötigt.

`AWSResourceAccessManagerResourceShareParticipantAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceAccessManagerResourceShareParticipantAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Dezember 2019, 20:41 UTC
- Bearbeitete Zeit: 9. Dezember 2019, 20:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceAccessManagerResourceShareParticipantAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",
        "ram:RejectResourceShareInvitation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceAccessManagerServiceRolePolicy

Beschreibung: Richtlinie, die den schreibgeschützten AWS Resource Access Manager auf die Organisationsstruktur der Kunden vorsieht. Sie enthält auch IAM-Berechtigungen für das eigenständige Löschen der Rolle.

`AWSResourceAccessManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 19:28 UTC
- Zeit bearbeitet: 14. November 2018, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceAccessManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
```

```
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerFullAccess

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen für den Zugriff auf Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

`AWSResourceExplorerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceExplorerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 7. November 2022, 20:01 UTC
- Bearbeitete Zeit: 14. November 2023, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerConsoleFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
```

```
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerOrganizationsAccess

Beschreibung: Diese Richtlinie gewährt Resource Explorer Administratorberechtigungen und anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen. Der AWS Organisationsadministrator benötigt diese Berechtigungen, um die Suche mit mehreren Konten in der Konsole einzurichten und zu verwalten.

`AWSResourceExplorerOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceExplorerOrganizationsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. November 2023, 17:01 UTC
- Bearbeitete Zeit: 14. November 2023, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:*",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ResourceExplorerGetSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer"
    },
    {
```

```
      "Sid" : "ResourceExplorerCreateSLRAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationsAdministratorAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Leseberechtigungen zum Suchen und Anzeigen von Resource Explorer-Ressourcen und gewährt anderen AWS Diensten zur Unterstützung dieses Zugriffs nur Leseberechtigungen.

`AWSResourceExplorerReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSResourceExplorerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. November 2022, 19:56 UTC
- Bearbeitete Zeit: 14. November 2023, 16:43 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceExplorerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Get*",
```

```
        "resource-explorer-2:List*",
        "resource-explorer-2:Search",
        "resource-explorer-2:BatchGetView",
        "ec2:DescribeRegions",
        "ram:ListResources",
        "ram:GetResourceShares",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceExplorerServiceRolePolicy

Beschreibung: Ermöglicht Resource Explorer, Ressourcen und CloudTrail Ereignisse in Ihrem Namen anzuzeigen, um Ihre Ressourcen für die Suche zu indizieren.

`AWSResourceExplorerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Oktober 2022, 20:35 UTC
- Bearbeitete Zeit: 16. Dezember 2025, 20:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSResourceExplorerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v22 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:DeleteIndex"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudTrailEventsAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/resource-
explorer-2/*"
    },
    {
      "Sid" : "ApiGatewayAccess",
      "Effect" : "Allow",
      "Action" : "apigateway:GET",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*"
      ]
    },
    {
      "Sid" : "ResourceInventoryAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "acm-pca:ListCertificateAuthorities",
        "acm:ListCertificates",
        "airflow:ListEnvironments",
```

```
        "amplify:ListApps",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "aoss:ListCollections",
        "app-integrations:ListApplications",
        "app-integrations:ListEventIntegrations",
        "appconfig:ListApplications",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensionAssociations",
        "appflow:ListFlows",
        "appmesh:ListGatewayRoutes",
        "appmesh:ListMeshes",
        "appmesh:ListRoutes",
        "appmesh:ListVirtualGateways",
        "appmesh:ListVirtualNodes",
        "appmesh:ListVirtualRouters",
        "appmesh:ListVirtualServices",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListServices",
        "apprunner:ListVpcConnectors",
        "appstream:DescribeAppBlocks",
        "appstream:DescribeApplications",
        "appstream:DescribeFleets",
        "appstream:DescribeImageBuilders",
        "appstream:DescribeStacks",
        "appsync:ListGraphqlApis",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListWorkspaces",
        "athena:ListDataCatalogs",
        "athena:ListWorkGroups",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessments",
        "autoscaling:DescribeAutoScalingGroups",
        "backup-gateway:ListHypervisors",
        "backup:ListBackupPlans",
        "backup:ListBackupVaults",
        "backup:ListReportPlans",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "batch:DescribeJobQueues",
        "batch:ListSchedulingPolicies",
        "bedrock:ListAgentAliases",
```

```
        "bedrock:ListAgents",
        "bedrock:ListDataAutomationProjects",
        "bedrock:ListFlows",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "chime:ListAppInstanceBots",
        "chime:ListAppInstanceUsers",
        "chime:ListAppInstances",
        "chime:ListMediaInsightsPipelineConfigurations",
        "chime:ListMediaPipelineKinesisVideoStreamPools",
        "chime:ListMediaPipelines",
        "chime:ListSipMediaApplications",
        "chime:ListVoiceConnectors",
        "cloud9:ListEnvironments",
        "cloudformation:ListResources",
        "cloudformation:ListStackSets",
        "cloudformation:ListStacks",
        "cloudfront:ListCachePolicies",
        "cloudfront:ListCloudFrontOriginAccessIdentities",
        "cloudfront:ListContinuousDeploymentPolicies",
        "cloudfront:ListDistributions",
        "cloudfront:ListFieldLevelEncryptionConfigs",
        "cloudfront:ListFieldLevelEncryptionProfiles",
        "cloudfront:ListFunctions",
        "cloudfront:ListOriginAccessControls",
        "cloudfront:ListOriginRequestPolicies",
        "cloudfront:ListRealtimeLogConfigs",
        "cloudfront:ListResponseHeadersPolicies",
        "cloudtrail:ListChannels",
        "cloudtrail:ListDashboards",
        "cloudtrail:ListEventDataStores",
        "cloudtrail:ListTrails",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeInsightRules",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListMetricStreams",
        "codeartifact:ListDomains",
        "codeartifact:ListRepositories",
        "codebuild:ListProjects",
```

```
        "codecommit:ListRepositories",
        "codeconnections:ListConnections",
        "codedeploy:ListApplications",
        "codedeploy:ListDeploymentConfigs",
        "codeguru-profiler:ListProfilingGroups",
        "codeguru-reviewer:ListRepositoryAssociations",
        "codepipeline:ListPipelines",
        "codepipeline:ListWebhooks",
        "codestar-connections:ListConnections",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "comprehend:ListDocumentClassifiers",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListFlywheels",
        "config:DescribeConfigRules",
        "connect:ListEvaluationForms",
        "connect:ListHoursOfOperations",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListPhoneNumbersV2",
        "connect:ListPrompts",
        "connect:ListQuickConnects",
        "connect:ListRoutingProfileQueues",
        "connect:ListRoutingProfiles",
        "connect:ListRules",
        "connect:ListSecurityProfiles",
        "connect:ListTaskTemplates",
        "connect:ListUsers",
        "databrew:ListDatasets",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "dataexchange:ListDataSets",
        "datapipeline:ListPipelines",
        "datasync:ListLocations",
        "datasync:ListTasks",
        "dax:DescribeClusters",
        "detective:ListGraphs",
        "devicefarm:ListInstanceProfiles",
        "devicefarm:ListProjects",
        "devicefarm:ListTestGridProjects",
        "directconnect:DescribeDirectConnectGateways",
```

```
        "dms:DescribeCertificates",
        "dms:DescribeEndpoints",
        "dms:DescribeEventSubscriptions",
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationSubnetGroups",
        "dms:DescribeReplicationTasks",
        "ds:DescribeDirectories",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeCapacityReservationFleets",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFleets",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeFpgaImages",
        "ec2:DescribeHostReservations",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceConnectEndpoints",
        "ec2:DescribeInstanceEventWindows",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:DescribeIpamResourceDiscoveries",
        "ec2:DescribeIpamResourceDiscoveryAssociations",
        "ec2:DescribeIpamScopes",
        "ec2:DescribeIpams",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInsightsAccessScopeAnalyses",
        "ec2:DescribeNetworkInsightsAccessScopes",
        "ec2:DescribeNetworkInsightsAnalyses",
        "ec2:DescribeNetworkInsightsPaths",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeReservedInstances",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSubnets",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnectPeers",
        "ec2:DescribeTransitGatewayMulticastDomains",
        "ec2:DescribeTransitGatewayPolicyTables",
        "ec2:DescribeTransitGatewayRouteTableAnnouncements",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVerifiedAccessEndpoints",
        "ec2:DescribeVerifiedAccessGroups",
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessTrustProviders",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetSubnetCidrReservations",
        "ecr-public:DescribeRepositories",
        "ecr:DescribeRepositories",
        "ecs:DescribeCapacityProviders",
        "ecs:DescribeServices",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTaskDefinitions",
        "eks:DescribeAccessEntry",
        "eks:DescribeAddon",
        "eks:DescribeFargateProfile",
        "eks:DescribeIdentityProviderConfig",
        "eks:DescribeNodegroup",
        "eks:ListAccessEntries",
```

```
        "eks:ListAddons",
        "eks:ListClusters",
        "eks:ListEksAnywhereSubscriptions",
        "eks:ListFargateProfiles",
        "eks:ListIdentityProviderConfigs",
        "eks:ListNodegroups",
        "eks:ListPodIdentityAssociations",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeCacheParameterGroups",
        "elasticache:DescribeCacheSubnetGroups",
        "elasticache:DescribeGlobalReplicationGroups",
        "elasticache:DescribeReplicationGroups",
        "elasticache:DescribeReservedCacheNodes",
        "elasticache:DescribeSnapshots",
        "elasticache:DescribeUserGroups",
        "elasticache:DescribeUsers",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticmapreduce:ListClusters",
        "emr-containers:ListJobTemplates",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListSecurityConfigurations",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:ListApplications",
        "es:ListDomainNames",
        "events:ListApiDestinations",
        "events:ListArchives",
        "events:ListConnections",
        "events:ListEndpoints",
        "events:ListEventBuses",
        "events:ListRules",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "finspace:ListEnvironments",
        "firehose:ListDeliveryStreams",
```

```
        "fis:ListExperimentTemplates",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetLabels",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetVariables",
        "fsx:DescribeBackups",
        "fsx:DescribeFileSystems",
        "gamelift:DescribeGameSessionQueues",
        "gamelift:DescribeMatchmakingConfigurations",
        "gamelift:DescribeMatchmakingRuleSets",
        "gamelift:ListAliases",
        "gamelift:ListBuilds",
        "gamelift:ListLocations",
        "gamelift:ListScripts",
        "geo:ListMaps",
        "geo:ListPlaceIndexes",
        "geo:ListTrackers",
        "glacier:ListVaults",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:ListEndpointGroups",
        "globalaccelerator:ListListeners",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetJobs",
        "glue:GetTables",
        "glue:GetTriggers",
        "glue:ListDataQualityRulesets",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "grafana:ListWorkspaces",
        "greengrass:ListComponentVersions",
```

```
        "greengrass:ListComponents",
        "greengrass:ListConnectorDefinitions",
        "greengrass:ListCoreDefinitions",
        "greengrass:ListDeviceDefinitions",
        "greengrass:ListFunctionDefinitions",
        "greengrass:ListGroups",
        "greengrass:ListLoggerDefinitions",
        "greengrass:ListResourceDefinitions",
        "greengrass:ListSubscriptionDefinitions",
        "groundstation:ListConfigs",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListMissionProfiles",
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:ListIPSets",
        "guardduty:ListMalwareProtectionPlans",
        "guardduty:ListPublishingDestinations",
        "guardduty:ListThreatIntelSets",
        "healthlake:ListFHIRDatastores",
        "iam:ListGroups",
        "iam:ListInstanceProfiles",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:ListUsers",
        "iam:ListVirtualMFADevices",
        "imagebuilder:ListComponentBuildVersions",
        "imagebuilder:ListComponents",
        "imagebuilder:ListContainerRecipes",
        "imagebuilder:ListDistributionConfigurations",
        "imagebuilder:ListImageBuildVersions",
        "imagebuilder:ListImagePipelines",
        "imagebuilder:ListImageRecipes",
        "imagebuilder:ListImages",
        "imagebuilder:ListInfrastructureConfigurations",
        "inspector2:ListFilters",
        "inspector:ListAssessmentTemplates",
        "iot:ListAuthorizers",
        "iot:ListBillingGroups",
        "iot:ListCACertificates",
        "iot:ListCertificates",
        "iot:ListFleetMetrics",
```

```
        "iot:ListJobTemplates",
        "iot:ListMitigationActions",
        "iot:ListPolicies",
        "iot:ListProvisioningTemplates",
        "iot:ListRoleAliases",
        "iot:ListScheduledAudits",
        "iot:ListSecurityProfiles",
        "iot:ListThingGroups",
        "iot:ListThingTypes",
        "iot:ListThings",
        "iot:ListTopicRuleDestinations",
        "iot:ListTopicRules",
        "iotanalytics:ListChannels",
        "iotanalytics:ListDatasets",
        "iotanalytics:ListDatastores",
        "iotanalytics:ListPipelines",
        "iotdeviceadvisor:ListSuiteDefinitions",
        "iotevents:ListAlarmModels",
        "iotevents:ListDetectorModels",
        "iotevents:ListInputs",
        "iotfleethub:ListApplications",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListVehicles",
        "iotsitewise:ListAccessPolicies",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListAssets",
        "iotsitewise:ListDashboards",
        "iotsitewise:ListGateways",
        "iotsitewise:ListPortals",
        "iotsitewise:ListProjects",
        "iottwinmaker:ListComponentTypes",
        "iottwinmaker:ListEntities",
        "iottwinmaker:ListSyncJobs",
        "iottwinmaker:ListWorkspaces",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
```

```
        "iotwireless:ListWirelessGateways",
        "ivs:ListChannels",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "kafka:ListClusters",
        "kafka:ListConfigurations",
        "kendra:ListAccessControlConfigurations",
        "kendra:ListDataSources",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListFeaturedResultsSets",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListThesauri",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kms:ListKeys",
        "lambda:ListCodeSigningConfigs",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "lex:ListBotAliases",
        "lex:ListBots",
        "license-manager:ListDistributedGrants",
        "lightsail:GetBuckets",
        "lightsail:GetCertificates",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "logs:DescribeDestinations",
        "logs:DescribeLogGroups",
        "logs:ListTagsForResource",
        "lookoutmetrics:ListAlerts",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:ListEnvironments",
        "macie2:ListAllowLists",
```

```
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindingsFilters",
        "managedblockchain:ListAccessors",
        "mediapackage-vod:ListAssets",
        "mediapackage-vod:ListPackagingConfigurations",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:ListChannels",
        "mediapackage:ListOriginEndpoints",
        "mediastore:ListContainers",
        "mediatailor:ListChannels",
        "mediatailor:ListLiveSources",
        "mediatailor:ListPlaybackConfigurations",
        "mediatailor:ListSourceLocations",
        "mediatailor:ListVodSources",
        "memorydb:DescribeACLs",
        "memorydb:DescribeClusters",
        "memorydb:DescribeParameterGroups",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "mobiletargeting:GetApps",
        "mobiletargeting:GetCampaigns",
        "mobiletargeting:GetSegments",
        "mobiletargeting:ListTemplates",
        "mq:ListBrokers",
        "mq:ListConfigurations",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetDevices",
        "networkmanager:GetLinks",
        "networkmanager:ListAttachments",
        "networkmanager:ListCoreNetworks",
        "oam:ListSinks",
        "omics:ListReferenceStores",
        "omics:ListRunGroups",
        "omics:ListWorkflows",
        "outposts:ListSites",
        "organizations:DescribeResourcePolicy",
        "organizations:ListPolicies",
        "panorama:ListPackages",
        "partnercentral:ListEngagementInvitations",
        "partnercentral:ListEngagements",
```

```
        "partnercentral:ListOpportunities",
        "partnercentral:ListResourceSnapshotJobs",
        "partnercentral:ListResourceSnapshots",
        "personalize:ListDatasetGroups",
        "personalize:ListDatasets",
        "personalize:ListSchemas",
        "personalize:ListSolutions",
        "pipes:ListPipes",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "profile:ListProfileObjectTypes",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentTemplates",
        "proton:ListServiceTemplates",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListLedgers",
        "quicksight:DescribeAccountSubscription",
        "quicksight:ListDataSets",
        "quicksight:ListDataSources",
        "quicksight:ListTemplates",
        "quicksight:ListThemes",
        "ram:GetResourceShares",
        "rds:DescribeBlueGreenDeployments",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyEndpoints",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeReservedDBInstances",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusters",
```

```
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeUsageLimits",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "rekognition:DescribeProjects",
        "resiliencehub:ListApps",
        "resiliencehub:ListResiliencyPolicies",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListViews",
        "resource-groups:ListGroups",
        "route53-recovery-control-config:ListClusters",
        "route53-recovery-control-config:ListControlPanels",
        "route53-recovery-control-config:ListRoutingControls",
        "route53-recovery-control-config:ListSafetyRules",
        "route53-recovery-readiness:ListCells",
        "route53-recovery-readiness:ListReadinessChecks",
        "route53-recovery-readiness:ListRecoveryGroups",
        "route53-recovery-readiness:ListResourceSets",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53domains:ListDomains",
        "route53resolver:ListFirewallDomainLists",
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverRules",
        "rum:ListAppMonitors",
        "s3:GetBucketLocation",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListStorageLensConfigurations",
        "s3:ListStorageLensGroups",
        "s3express:ListAllMyDirectoryBuckets",
        "sagemaker:ListActions",
        "sagemaker:ListAlgorithms",
        "sagemaker:ListAppImageConfigs",
```

```
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListClusters",
        "sagemaker:ListCodeRepositories",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListExperiments",
        "sagemaker:ListFeatureGroups",
        "sagemaker:ListFlowDefinitions",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHumanTaskUis",
        "sagemaker:ListImageVersions",
        "sagemaker:ListImages",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListInferenceExperiments",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListModelCardVersions",
        "sagemaker:ListModelCards",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListMonitoringSchedules",
        "sagemaker:ListNotebookInstanceLifecycleConfigs",
        "sagemaker:ListNotebookInstances",
        "sagemaker:ListPipelines",
        "sagemaker:ListProjects",
        "sagemaker:ListSpaces",
        "sagemaker:ListStudioLifecycleConfigs",
        "sagemaker:ListTrialComponents",
        "sagemaker:ListTrials",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListWorkforces",
        "sagemaker:ListWorkteams",
        "scheduler:ListScheduleGroups",
        "schemas:ListDiscoverers",
        "secretsmanager:ListSecrets",
        "servicecatalog:ListApplications",
        "servicecatalog:ListAttributeGroups",
        "servicediscovery:ListServices",
        "ses:ListConfigurationSets",
        "ses:ListContactLists",
```

```
        "ses:ListDedicatedIpPools",
        "ses:ListEmailIdentities",
        "shield:ListProtectionGroups",
        "shield:ListProtections",
        "signer:ListSigningProfiles",
        "sns:ListTopics",
        "sqs:ListQueues",
        "ssm-incidents:ListResponsePlans",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeMaintenanceWindowTargets",
        "ssm:DescribeMaintenanceWindowTasks",
        "ssm:DescribeMaintenanceWindows",
        "ssm:DescribeParameters",
        "ssm:DescribeSessions",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "ssm:ListResourceDataSync",
        "states:ListActivities",
        "states:ListStateMachines",
        "storagegateway:ListGateways",
        "synthetics:DescribeCanaries",
        "synthetics:ListGroups",
        "transfer:ListAgreements",
        "transfer:ListCertificates",
        "transfer:ListConnectors",
        "transfer:ListProfiles",
        "transfer:ListServers",
        "transfer:ListUsers",
        "transfer:ListWorkflows",
        "verifiedpermissions:ListPolicyStores",
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTargetGroups",
        "wafv2:ListIPSets",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListRuleGroups",
        "wafv2:ListWebACLs",
        "wisdom:ListAssistantAssociations",
        "wisdom:ListAssistants",
        "wisdom:ListContents",
        "wisdom:ListKnowledgeBases",
        "workspaces-web:ListPortals",
```

```
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsForReadGetResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetKnowledgeBase",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentCollaborators",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListTagsForResource",
        "cloudformation:GetResource",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetResourcePolicy",
        "dynamodb:ListTagsOfResource",
        "ecs:DescribeClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTagsForResource",
        "eks:DescribeCluster",
        "elasticloadbalancing:DescribeCapacityReservation",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetHealth",
        "events:DescribeRule",
        "events:ListTagsForResource",
        "events:ListTargetsByRule",
        "iam:GetPolicy",
```

```
            "iam:GetPolicyVersion",
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "kinesis:DescribeStreamSummary",
            "kinesis:ListTagsForStream",
            "lambda:GetEventSourceMapping",
            "lambda:GetFunction",
            "lambda:GetFunctionCodeSigningConfig",
            "lambda:GetFunctionRecursionConfig",
            "lambda:GetRuntimeManagementConfig",
            "lambda:ListTags",
            "logs:DescribeIndexPolicies",
            "logs:DescribeResourcePolicies",
            "logs:GetDataProtectionPolicy",
            "route53:GetHostedZone",
            "route53:ListQueryLoggingConfigs",
            "route53:ListTagsForResource",
            "s3:GetAccelerateConfiguration",
            "s3:GetAnalyticsConfiguration",
            "s3:GetBucketCORS",
            "s3:GetBucketLogging",
            "s3:GetBucketMetadataTableConfiguration",
            "s3:GetBucketNotification",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketOwnershipControls",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketTagging",
            "s3:GetBucketVersioning",
            "s3:GetBucketWebsite",
            "s3:GetEncryptionConfiguration",
            "s3:GetIntelligentTieringConfiguration",
            "s3:GetInventoryConfiguration",
            "s3:GetLifecycleConfiguration",
            "s3:GetMetricsConfiguration",
            "s3:GetReplicationConfiguration",
            "sagemaker:DescribeEndpoint",
            "sagemaker:ListTags",
            "sns:GetDataProtectionPolicy",
            "sns:GetTopicAttributes",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTagsForResource",
            "sqs:GetQueueAttributes",
```

```
        "sqs:ListQueueTags"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSResourceGroupsReadOnlyAccess

Beschreibung: Dies ist die schreibgeschützte Richtlinie für AWS Resource Groups

`AWSResourceGroupsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSResourceGroupsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 10:27 UTC
- Bearbeitete Zeit: 5. Februar 2019, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "tag:Get*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "elasticache:DescribeCacheClusters",
        "elasticache:DescribeSnapshots",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListClusters",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:ListTagsForVault",
        "kinesis:ListStreams",
        "kinesis:DescribeStream",
        "kinesis:ListTagsForStream",
        "opsworks:DescribeStacks",
        "opsworks:ListTags",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "route53domains:ListDomains",
        "route53:ListHealthChecks",
        "route53:GetHealthCheck",
```

```
        "route53:ListHostedZones",
        "route53:GetHostedZone",
        "route53:ListTagsForResource",
        "storagegateway:ListGateways",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:ListTagsForResource",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags",
        "ssm:ListDocuments"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMaker_FullAccess

Beschreibung: Bietet vollen Zugriff auf AWS RoboMaker über das AWS-Managementkonsole und SDK. Bietet auch ausgewählten Zugriff auf verwandte Dienste (z. B. S3, IAM).

`AWSRoboMaker_FullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRoboMaker_FullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 10. September 2020, 18:34 UTC
- Bearbeitete Zeit: 16. September 2021, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMaker_FullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "robomaker:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr:BatchGetImage",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecr-public:DescribeImages",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "robomaker.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "robomaker.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS RoboMaker über das AWS-Managementkonsole und SDK

`AWSRoboMakerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRoboMakerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2018, 05:30 Uhr UTC
- Bearbeitete Zeit: 28. August 2020, 23:10 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "robomaker:List*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerServicePolicy

Beschreibung: RoboMaker Servicerichtlinie

`AWSRoboMakerServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 06:30 Uhr UTC
- Bearbeitete Zeit: 11. November 2021, 22:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRoboMakerServicePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction",
        "robomaker:CreateSimulationJob",
        "robomaker:CancelSimulationJob"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "robomaker:TagResource"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:robomaker:*:*:simulation-job/*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration",
        "lambda:DeleteFunction",
```

```
        "lambda:ListVersionsByFunction",
        "lambda:GetAlias",
        "lambda:UpdateAlias",
        "lambda:CreateAlias",
        "lambda:DeleteAlias"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "robomaker.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRoboMakerServiceRolePolicy

Beschreibung: RoboMaker Servicerichtlinie

`AWSRoboMakerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRoboMakerServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. November 2018, 05:33 UTC
- Bearbeitete Zeit: 26. November 2018, 05:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRoboMakerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "greengrass:CreateDeployment",
        "greengrass:CreateGroupVersion",
        "greengrass:CreateFunctionDefinition",
        "greengrass:CreateFunctionDefinitionVersion",
        "greengrass:GetDeploymentStatus",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetFunctionDefinitionVersion",
        "greengrass:GetAssociatedRole",
        "lambda:CreateFunction"
```

```
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "lambda:UpdateFunctionCode",
        "lambda:GetFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:lambda:*:*:function:aws-robomaker-*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRolesAnywhereFullAccess

Beschreibung: Stellt alle Berechtigungen für IAM Roles Anywhere-Ressourcen bereit, einschließlich, aber nicht beschränkt auf: CreateProfile,, DeleteTrustAnchor DisableCRL,. ResetNotificationSettings

`AWSRolesAnywhereFullAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSRolesAnywhereFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Juli 2025, 14:52 UTC
- Bearbeitete Zeit: 16. Juli 2025, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:CreateTrustAnchor",
        "rolesanywhere:DeleteTrustAnchor",
        "rolesanywhere:DisableTrustAnchor",
        "rolesanywhere:EnableTrustAnchor",
        "rolesanywhere:UpdateTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
```

```
    },
    {
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile",
        "rolesanywhere:CreateProfile",
        "rolesanywhere:DeleteProfile",
        "rolesanywhere:DisableProfile",
        "rolesanywhere:EnableProfile",
        "rolesanywhere:UpdateProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl",
        "rolesanywhere:DeleteCrl",
        "rolesanywhere:DisableCrl",
        "rolesanywhere:EnableCrl",
        "rolesanywhere:ImportCrl",
        "rolesanywhere:UpdateCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
```

```
    {
      "Sid" : "OtherRolesAnywherePermissions",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:PutAttributeMapping",
        "rolesanywhere:DeleteAttributeMapping",
        "rolesanywhere:ResetNotificationSettings",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:TagResource",
        "rolesanywhere:UntagResource",
        "rolesanywhere:PutNotificationSettings"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToRolesAnywhere",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "rolesanywhere.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateRolesAnywhereServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "rolesanywhere.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRolesAnywhereReadOnly

Beschreibung: Stellt nur Leseberechtigungen für IAM Roles Anywhere-Ressourcen bereit, einschließlich, aber nicht beschränkt auf: GetTrustAnchor,, ListProfiles GetCRL. In dieser Richtlinie sind keine weiteren Berechtigungen für andere Dienste enthalten.

`AWSRolesAnywhereReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSRolesAnywhereReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Juli 2025, 15:07 UTC
- Bearbeitete Zeit: 16. Juli 2025, 15:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSRolesAnywhereReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "Profiles",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListProfiles",
        "rolesanywhere:GetProfile"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:profile/*"
      ]
    },
    {
      "Sid" : "CRLs",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListCrls",
        "rolesanywhere:GetCrl"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:crl/*"
      ]
    },
    {
      "Sid" : "Subjects",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListSubjects",
        "rolesanywhere:GetSubject"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:subject/*"
      ]
    },
    {
      "Sid" : "TrustAnchors",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTrustAnchors",
        "rolesanywhere:GetTrustAnchor"
      ],
      "Resource" : [
        "arn:aws:rolesanywhere:*:*:trust-anchor/*"
      ]
    },
    {
```

```
      "Sid" : "Tags",
      "Effect" : "Allow",
      "Action" : [
        "rolesanywhere:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSRolesAnywhereServicePolicy

Beschreibung: Ermöglicht IAM Roles Anywhere, service/usage Metriken an private Zertifizierungsstellen zu veröffentlichen CloudWatch und deren Status in Ihrem Namen zu überprüfen.

`AWSRolesAnywhereServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Juli 2022, 15:26 UTC
- Bearbeitete Zeit: 5. Juli 2022, 15:26 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSRolesAnywhereServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/RolesAnywhere",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:GetCertificateAuthorityCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "arn:aws:acm-pca:*:*:*"
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSS3OnOutpostsServiceRolePolicy

Beschreibung: Erlauben Sie dem Amazon S3 on Outposts-Service, EC2 Netzwerkressourcen in Ihrem Namen zu verwalten.

`AWSS3OnOutpostsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Oktober 2023, 20:32 UTC
- Bearbeitete Zeit: 3. Oktober 2023, 20:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSS3OnOutpostsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource" : "*",
      "Sid" : "DescribeVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Sid" : "CreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
```

```
      },
      "Sid" : "CreateTagsForCreateNetworkInterface"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:ipv4pool-ec2/*"
      ],
      "Sid" : "AllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "S3 On Outposts"
        }
      },
      "Sid" : "CreateTagsForAllocateIpAddress"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DisassociateAddress",
        "ec2:ReleaseAddress",
        "ec2:AssociateAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "S3 On Outposts"
        }
```

```
      },
      "Sid" : "ReleaseVpcResources"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateNetworkInterface",
            "AllocateAddress"
          ],
          "aws:RequestTag/CreatedBy" : [
            "S3 On Outposts"
          ]
        }
      },
      "Sid" : "CreateTags"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSavingsPlansFullAccess

Beschreibung: Bietet vollen Zugriff auf den Savings Plans-Service

`AWSSavingsPlansFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSavingsPlansFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "savingsplans:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSavingsPlansReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den Savings Plans-Service

`AWSSavingsPlansReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSavingsPlansReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. November 2019, 22:45 UTC
- Bearbeitete Zeit: 6. November 2019, 22:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSavingsPlansReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "savingsplans:Describe*",
        "savingsplans:List*"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecretsManagerClientReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf das Abrufen und Beschreiben von Geheimnissen aus Secrets Manager. Diese Richtlinie ermöglicht auch die Entschlüsselung von KMS-Schlüsseln für Secrets Manager Manager-Geheimnisse.

`AWSSecretsManagerClientReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecretsManagerClientReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. November 2025, 20:04 UTC
- Bearbeitete Zeit: 5. November 2025, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecretsManagerClientReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerGetAndDescribeSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*"
    },
    {
      "Sid" : "KMSDecryptKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:*:secret:*",
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubFullAccess

Beschreibung: Bietet vollen Zugriff auf die Nutzung von AWS Security Hub.

`AWSSecurityHubFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityHubFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 23:54 UTC
- Zeit bearbeitet: 21. November 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubAllowAll",
      "Effect" : "Allow",
      "Action" : "securityhub:*",
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceLinkedRole",
      "Effect" : "Allow",
```

```
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "securityhub.amazonaws.com",
            "securityhubv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OtherServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "guardduty:UpdateDetector",
        "guardduty:EnableOrganizationAdminAccount",
        "guardduty:ListOrganizationAdminAccounts",
        "guardduty:DeleteDetector",
        "guardduty:CreateDetector",
        "guardduty:CreateMembers",
        "guardduty:UpdateOrganizationConfiguration",
        "guardduty:DescribeOrganizationConfiguration",
        "inspector2:BatchGetAccountStatus",
        "inspector2:Enable",
        "inspector2:Disable",
        "inspector2:EnableDelegatedAdminAccount",
        "inspector2:DisableDelegatedAdminAccount",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:UpdateOrganizationConfiguration",
        "inspector2:DescribeOrganizationConfiguration",
        "pricing:GetProducts",
        "account:ListRegions",
        "account:GetRegionOptStatus",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubOrganizationsAccess

Beschreibung: Erteilt die Erlaubnis, AWS Security Hub innerhalb einer Organisation zu aktivieren und zu verwalten. Beinhaltet die unternehmensweite Aktivierung des Dienstes und die Festlegung des delegierten Administratorkontos für den Dienst.

`AWSSecurityHubOrganizationsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityHubOrganizationsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. März 2021, 20:53 UTC
- Bearbeitete Zeit: 21. November 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubOrganizationsAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationPermissionsEnable",
      "Effect" : "Allow",
      "Action" : "organizations:EnableAWSServiceAccess",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Sid" : "OrganizationPermissionsDelegatedAdmin",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:account/o-*/*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com",
            "inspector2.amazonaws.com",
            "guardduty.amazonaws.com",
            "malware-protection.guardduty.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource" : [
        "arn:aws:organizations::*:root/o-*/*",
        "arn:aws:organizations::*:account/o-*/*",
        "arn:aws:organizations::*:ou/o-*/*",
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
```

```
          "organizations:PolicyType" : [
            "SECURITYHUB_POLICY",
            "INSPECTOR_POLICY"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationPolicyTaggingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:TagResource",
        "organizations:UntagResource",
        "organizations:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:organizations::*:policy/o-*/securityhub_policy/*",
        "arn:aws:organizations::*:policy/o-*/inspector_policy/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Security Hub Hub-Ressourcen

`AWSSecurityHubReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityHubReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. November 2018, 01:34 UTC
- Bearbeitete Zeit: 22. Februar 2024, 23:45 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityHubReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSecurityHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubServiceRolePolicy

Beschreibung: Eine dienstbezogene Rolle, die AWS Security Hub benötigt, um auf Ihre Ressourcen zugreifen zu können.

`AWSSecurityHubServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2018, 23:47 UTC
- Bearbeitete Zeit: 27. November 2023, 03:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "SecurityHubServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmsForMetric",
        "logs:DescribeMetricFilters",
        "sns:ListSubscriptionsByTopic",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "iam:GenerateCredentialReport",
        "organizations:ListAccounts",
        "config:PutEvaluations",
        "tag:GetResources",
        "iam:GetCredentialReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "securityhub:BatchDisableStandards",
        "securityhub:BatchEnableStandards",
        "securityhub:BatchUpdateStandardsControlAssociations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:CreateMembers",
        "securityhub:DeleteMembers",
        "securityhub:DescribeHub",
        "securityhub:DescribeOrganizationConfiguration",
        "securityhub:DescribeStandards",
        "securityhub:DescribeStandardsControls",
        "securityhub:DisassociateFromAdministratorAccount",
        "securityhub:DisassociateMembers",
        "securityhub:DisableSecurityHub",
        "securityhub:EnableSecurityHub",
        "securityhub:GetEnabledStandards",
```

```
        "securityhub:ListStandardsControlAssociations",
        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubServiceRoleConfigPermissions",
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
    },
    {
      "Sid" : "SecurityHubServiceRoleOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityHubV2ServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es Security Hub, AWS Konfigurationsregeln und Security Hub Hub-Ressourcen in Ihrer Organisation und in Ihrem Namen zu verwalten.

`AWSSecurityHubV2ServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juni 2025, 17:37 UTC
- Zeit bearbeitet: 17. November 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityHubV2ServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsConfig",
      "Effect" : "Allow",
      "Action" : [
```

```
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder"
      ],
      "Resource" : [
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssets/*",
        "arn:aws:config:*:*:configuration-recorder/
AWSConfigurationRecorderForSecurityHubAssetsGlobal/*"
      ]
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleAssetsIamPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleSecurityHubPermissions",
      "Effect" : "Allow",
      "Action" : [
        "securityhub:DisableSecurityHubV2",
        "securityhub:EnableSecurityHubV2",
        "securityhub:DescribeSecurityHubV2"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hubv2/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleTagPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsOnResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:aws:organizations::*:*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleOrganizationsPermissionsWithoutResources",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleDelegatedAdminPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "securityhub.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleEcrListingPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ecr:DescribeImages",
        "ecr:DescribeRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaMetricPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleLambdaListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityHubV2ServiceRoleIamListingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetAccountSummary"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityIncidentResponseCaseFullAccess

Beschreibung: Die Richtlinie gewährt Kunden Lese- und Schreibberechtigungen für Fallressourcen, die über den Security Incident Response Service erstellt wurden.

`AWSSecurityIncidentResponseCaseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityIncidentResponseCaseFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2024, 23:21 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseCaseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRCaseReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
```

```
        "security-ir:ListComments",
        "security-ir:ListCaseEdits"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRCaseTagReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIRCaseWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityIRCaseTagWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:UntagResource"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityIncidentResponseFullAccess

Beschreibung: Die Richtlinie gewährt Kunden Lese- und Schreibberechtigungen für alle Ressourcen, die dem Security Incident Response Service zugeordnet sind.

`AWSSecurityIncidentResponseFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityIncidentResponseFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2024, 23:21 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 23:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIRWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateMembership",
        "security-ir:UpdateMembership",
        "security-ir:CancelMembership",
        "security-ir:CreateCase",
        "security-ir:UpdateCase",
        "security-ir:CloseCase",
        "security-ir:UpdateCaseStatus",
        "security-ir:UpdateResolverType",
        "security-ir:GetCaseAttachmentUploadUrl",
        "security-ir:CreateCaseComment",
        "security-ir:UpdateCaseComment",
        "security-ir:TagResource",
        "security-ir:UntagResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "aws:MultiFactorAuthPresent" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponse",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForSecurityIncidentResponseTriage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/triage.security-ir.amazonaws.com/
AWSServiceRoleForSecurityIncidentResponse_Triage"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityIncidentResponseReadOnlyAccess

Beschreibung: Die Richtlinie gewährt Kunden nur Leseberechtigungen für alle Ressourcen, die dem Security Incident Response Service zugeordnet sind. Die Berechtigung umfasst GetCaseAttachmentDownloadUrl auch den Zugriff auf die Möglichkeit, Fallanhänge herunterzuladen. URLs

`AWSSecurityIncidentResponseReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSecurityIncidentResponseReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2024, 23:06 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 23:06 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSecurityIncidentResponseReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIRReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:BatchGetMemberAccountDetails",
        "security-ir:GetMembership",
        "security-ir:ListMemberships",
        "security-ir:GetCase",
        "security-ir:ListCases",
        "security-ir:GetCaseAttachmentDownloadUrl",
        "security-ir:ListComments",
        "security-ir:ListCaseEdits",
        "security-ir:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityIncidentResponseServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die von Security Incident Response verwaltet oder genutzt werden

`AWSSecurityIncidentResponseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2024, 16:36 UTC
- Bearbeitete Zeit: 21. November 2025, 04:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecurityIncidentResponseOrganizationsPolicy",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecurityIncidentResponseCreateCasePolicyTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:TagResource",
        "security-ir:CreateCase"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      },
      "Resource" : "arn:aws:security-ir:*:*:case/*"
    },
    {
      "Sid" : "SecurityIncidentResponseOperationsPolicy",
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetCase",
        "security-ir:UpdateCase",
        "security-ir:ListCases",
        "security-ir:CreateCaseComment",
        "security-ir:ListComments"
      ],
      "Resource" : "arn:aws:security-ir:*:*:case/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSecurityIncidentResponseTriageServiceRolePolicy

Beschreibung: Bietet Zugriff auf AWS Security Incident Response, um Ihre Umgebung kontinuierlich auf Sicherheitsbedrohungen zu überwachen, Sicherheitsdienste so zu optimieren, dass Warnmeldungen reduziert werden, und Informationen zur Untersuchung potenzieller Vorfälle zu sammeln.

`AWSSecurityIncidentResponseTriageServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2024, 16:36 UTC
- Bearbeitete Zeit: 2. Juni 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSecurityIncidentResponseTriageServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "triage.security-ir.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "guardduty:ArchiveFindings",
        "guardduty:CreateFilter",
        "guardduty:DescribeMalwareScans",
        "guardduty:GetAdministratorAccount",
        "guardduty:GetDetector",
        "guardduty:GetFilter",
        "guardduty:GetFindings",
```

```
        "guardduty:ListDetectors",
        "guardduty:ListFilters",
        "guardduty:StartMalwareScan",
        "guardduty:UpdateFindingsFeedback"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:BatchUpdateFindings",
        "securityhub:DescribeHub",
        "securityhub:GetEnabledStandards",
        "securityhub:GetFindings",
        "securityhub:ListEnabledProductsForImport",
        "securityhub:UpdateFindings"
      ],
      "Resource" : "arn:aws:securityhub:*:*:hub/default"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:CreateCase",
        "security-ir:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SecurityIncidentResponseManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/SecurityIncidentResponseManaged" : "true",
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:UpdateCase"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SecurityIncidentResponseManaged" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "security-ir:GetMembership",
        "security-ir:ListMemberships"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAdminFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltungsfunktionen des Servicekatalogs

`AWSServiceCatalogAdminFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogAdminFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Februar 2018, 17:19 Uhr UTC
- Bearbeitete Zeit: 13. April 2023, 18:43 UTC

- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
```

```
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateUploadBucket",
        "cloudformation:GetTemplateSummary",
        "cloudformation:ValidateTemplate",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicecatalog:List*",
        "servicecatalog:TagResource",
        "servicecatalog:UntagResource",
        "servicecatalog:SyncResource",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:Accept*",
        "servicecatalog:Associate*",
        "servicecatalog:Batch*",
```

```
        "servicecatalog:Copy*",
        "servicecatalog:Create*",
        "servicecatalog:Delete*",
        "servicecatalog:Describe*",
        "servicecatalog:Disable*",
        "servicecatalog:Disassociate*",
        "servicecatalog:Enable*",
        "servicecatalog:Execute*",
        "servicecatalog:Import*",
        "servicecatalog:Provision*",
        "servicecatalog:Put*",
        "servicecatalog:Reject*",
        "servicecatalog:Terminate*",
        "servicecatalog:Update*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "servicecatalog.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "orgsdatasync.servicecatalog.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAdminReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Administratorfunktionen von Service Catalog

`AWSServiceCatalogAdminReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogAdminReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2019, 18:53 Uhr UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAdminReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "iam:GetGroup",
        "iam:GetRole",
        "iam:GetUser",
        "iam:ListGroups",
        "iam:ListRoles",
        "iam:ListUsers",
        "servicecatalog:Get*",
        "servicecatalog:List*",
        "servicecatalog:Describe*",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:Search*",
        "ssm:DescribeDocument",
```

```
        "ssm:GetAutomationExecution",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryFullAccess

Beschreibung: Bietet vollen Zugriff auf die Funktionen der Service Catalog App Registry

`AWSServiceCatalogAppRegistryFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogAppRegistryFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2020, 22:25 UTC
- Bearbeitete Zeit: 7. Dezember 2023, 21:50 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AppRegistryUpdateStackAndResourceGroupTagging",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "tag:GetResources"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryResourceGroupsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "resource-groups:GetGroupConfiguration",
        "resource-groups:AssociateResource",
        "resource-groups:DisassociateResource"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/AWS_*",
```

```
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AppRegistryOperations",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "servicecatalog:CreateApplication",
        "servicecatalog:GetApplication",
        "servicecatalog:UpdateApplication",
        "servicecatalog:DeleteApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:AssociateResource",
        "servicecatalog:DisassociateResource",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:CreateAttributeGroup",
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:SyncResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration",
        "servicecatalog:PutConfiguration"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppRegistryResourceTagging",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListTagsForResource",
        "servicecatalog:UntagResource",
        "servicecatalog:TagResource"
      ],
      "Resource" : "arn:aws:servicecatalog:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die Funktionen der Service Catalog App Registry

`AWSServiceCatalogAppRegistryReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogAppRegistryReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2020, 22:34 UTC

- Zeit bearbeitet: 17. November 2022, 18:16 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogAppRegistryReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:GetApplication",
        "servicecatalog:ListApplications",
        "servicecatalog:GetAssociatedResource",
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:ListAssociatedAttributeGroups",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:ListAttributeGroups",
        "servicecatalog:ListTagsForResource",
        "servicecatalog:ListAttributeGroupsForApplication",
        "servicecatalog:GetConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogAppRegistryServiceRolePolicy

Beschreibung: Ermöglicht Service Catalog AppRegistry , Resource Groups in Ihrem Namen zu verwalten

`AWSServiceCatalogAppRegistryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. Mai 2021, 22:18 Uhr UTC
- Bearbeitete Zeit: 26. Oktober 2022, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogAppRegistryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:DescribeStacks",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:GetTags",
        "resource-groups:Tag",
        "resource-groups:Untag"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroup",
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry*",
        "arn:*:resource-groups:*:*:group/AWS_CloudFormation_Stack*"
```

```
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogEndUserFullAccess

Beschreibung: Bietet vollen Zugriff auf die Funktionen des Servicekatalogs für Endbenutzer

`AWSServiceCatalogEndUserFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogEndUserFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. Februar 2018, 17:22 Uhr UTC
- Bearbeitete Zeit: 10. Juli 2019, 20:30 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DeleteChangeSet",
        "cloudformation:TagResource",
        "cloudformation:CreateStackSet",
        "cloudformation:CreateStackInstances",
        "cloudformation:UpdateStackSet",
        "cloudformation:UpdateStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:ProvisionProduct",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:TerminateProvisionedProduct",
        "servicecatalog:UpdateProvisionedProduct",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:CreateProvisionedProductPlan",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ExecuteProvisionedProductPlan",
        "servicecatalog:DeleteProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogEndUserReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Service Catalog-Endbenutzerfunktionen

`AWSServiceCatalogEndUserReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSServiceCatalogEndUserReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. Oktober 2019, 18:49 UTC
- Bearbeitete Zeit: 25. Oktober 2019, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSServiceCatalogEndUserReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackResources",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/SC-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
        "arn:aws:cloudformation:*:*:changeSet/SC-*",
        "arn:aws:cloudformation:*:*:stackset/SC-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplateSummary",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:SearchProducts",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DescribeProvisionedProduct",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ListStackInstancesForProvisionedProduct",
        "servicecatalog:ScanProvisionedProducts",
        "servicecatalog:SearchProvisionedProducts",
        "servicecatalog:DescribeProvisionedProductPlan",
        "servicecatalog:ListProvisionedProductPlans",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeServiceActionExecutionParameters"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "servicecatalog:userLevel" : "self"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogOrgsDataSyncServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rollenrichtlinie AWS ServiceCatalog zur Synchronisierung mit der Organisationsstruktur von AWS Organizations

`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. April 2023, 20:48 UTC
- Bearbeitete Zeit: 8. Dezember 2025, 19:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsDataSyncToServiceCatalogRegions",
      "Effect" : "Allow",
      "Action" : [
        "account:ListRegions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceCatalogSyncServiceRolePolicy

Beschreibung: Eine serviceverknüpfte Rolle AWS ServiceCatalog zum Synchronisieren von Bereitstellungsartefakten aus Quell-Repositorys

`AWSServiceCatalogSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 15. November 2022, 21:20 UTC
- Bearbeitete Zeit: 03. Mai 2024, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceCatalogSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ArtifactSyncToServiceCatalog",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListProvisioningArtifacts",
        "servicecatalog:DescribeProductAsAdmin",
        "servicecatalog:DeleteProvisioningArtifact",
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:DescribeProvisioningArtifact",
        "servicecatalog:CreateProvisioningArtifact",
        "servicecatalog:UpdateProvisioningArtifact"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessArtifactRepositories",
      "Effect" : "Allow",
      "Action" : [
        "codestar-connections:UseConnection",
        "codeconnections:UseConnection"
      ],
      "Resource" : [
```

```
        "arn:aws:codestar-connections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "ValidateTemplate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForAmazonEKSNodegroup

Beschreibung: Erforderliche Berechtigungen für die Verwaltung von Knotengruppen im Kundenkonto. Diese Richtlinien betrafen die Verwaltung der folgenden Ressourcen: AutoscalingGroups SecurityGroups, LaunchTemplates und. InstanceProfiles

`AWSServiceRoleForAmazonEKSNodegroup`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. November 2019, 01:34 UTC

- Zeit bearbeitet: 21. November 2024, 00:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonEKSNodegroup`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SharedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks" : "*"
        }
      }
    },
    {
      "Sid" : "EKSCreatedSecurityGroupRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeInstances",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "LaunchTemplateRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "AutoscalingRelatedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:TerminateInstanceInAutoScalingGroup",
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:PutLifecycleHook",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:EnableMetricsCollection",
        "autoscaling:PutScheduledUpdateGroupAction",
        "autoscaling:ResumeProcesses",
        "autoscaling:SuspendProcesses"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:*:autoScalingGroupName/eks-*"
    },
```

```
    {
      "Sid" : "AllowAutoscalingToCreateSLR",
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "autoscaling.amazonaws.com"
        }
      },
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowASGCreationByEKS",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:CreateAutoScalingGroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name"
          ]
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToAutoscaling",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowPassRoleToEC2",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsToManageResourcesForNodegroups",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "ec2:CreateLaunchTemplate",
        "ec2:DescribeInstances",
        "iam:GetInstanceProfile",
        "ec2:DescribeLaunchTemplates",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RunInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:GetConsoleOutput",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeCapacityReservations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PermissionsToCreateAndManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:AddRoleToInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/eks-*"
    },
    {
      "Sid" : "PermissionsToDeleteEKSAndKubernetesTags",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "PermissionsForManagedNodegroupsAutoRepair",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/eks:nodegroup-name" : "*"
        }
      }
    },
    {
      "Sid" : "PermissionsToCreateEKSAndKubernetesTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
```

```
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "AllowTaggingEC2ResourcesOnlyDuringInstanceCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:*:ec2:*:*:instance/*",
        "arn:*:ec2:*:*:volume/*",
        "arn:*:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        },
        "ForAnyValue:StringLike" : {
          "aws:TagKeys" : [
            "eks",
            "eks:cluster-name",
            "eks:nodegroup-name",
            "kubernetes.io/cluster/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForAmazonQDeveloper

Beschreibung: Diese serviceverknüpfte Rolle bietet Amazon Q Developer die Möglichkeit, Nutzungsinformationen bereitzustellen.

`AWSServiceRoleForAmazonQDeveloper`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. April 2024, 07:40 UTC
- Bearbeitete Zeit: 25. April 2024, 07:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAmazonQDeveloper`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Q"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForAWSTransform

Beschreibung: Diese dienstverknüpfte Rolle bietet AWS Transform die Möglichkeit, Nutzungsinformationen bereitzustellen.

`AWSServiceRoleForAWSTransform`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Mai 2025, 13:37 UTC
- Bearbeitete Zeit: 1. Dezember 2025, 13:19 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForAWSTransform`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Transform"
          ]
        }
      }
    },
    {
      "Sid" : "UserManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:ListApplicationAssignmentsForPrincipal"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SupportCaseManagement",
      "Effect" : "Allow",
      "Action" : [
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:AddCommunicationToCase",
        "support:ResolveCase"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ExternalIdpSecretsAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:transform!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "transform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy

Beschreibung: Bietet Zugriff auf Systems Manager Manager-Ressourcen, die von CloudWatch Alarms verwendet werden

`AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Oktober 2020, 09:49 UTC
- Zeit bearbeitet: 1. Oktober 2020, 09:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchAlarmsActionSSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePoli

Beschreibung: Ermöglicht CloudWatch den Zugriff auf RDS Performance Insights Insights-Metriken in Ihrem Namen

`AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2023, 09:32 UTC
- Bearbeitete Zeit: 7. September 2023, 09:32 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCloudWatchMetrics_DbPerfInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "pi:GetResourceMetrics"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCodeGuru-Profiler

Beschreibung: Eine servicebezogene Rolle, die Amazon CodeGuru Profiler benötigt, um Benachrichtigungen in Ihrem Namen zu versenden.

`AWSServiceRoleForCodeGuru-Profiler`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. Juni 2020, 22:04 UTC
- Bearbeitete Zeit: 26. Juni 2020, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeGuru-Profiler`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowSNSPublishToSendNotifications",
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForCodeWhispererPolicy

Beschreibung: Diese Rolle gewährt Berechtigungen für den CodeWhisperer Zugriff auf Daten in Ihrem Konto, um die Abrechnung zu berechnen, bietet Zugriff auf die Erstellung und den Zugriff auf Sicherheitsberichte in Amazon CodeGuru sowie die Übermittlung von Daten an CloudWatch.

`AWSServiceRoleForCodeWhispererPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. März 2023, 19:39 UTC
- Bearbeitete Zeit: 29. März 2024, 22:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForCodeWhispererPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "sid1",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "sid2",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListDirectoryAssociations",
        "sso:DescribeRegisteredRegions",
        "sso:GetProfile",
        "sso:GetManagedApplicationInstance",
        "sso:ListApplicationAssignments",
        "sso:DescribeInstance",
        "sso:DescribeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid3",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateUploadUrl"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "sid4",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:CreateScan",
        "codeguru-security:GetScan",
        "codeguru-security:ListFindings",
        "codeguru-security:GetFindings"
      ],
      "Resource" : [
        "arn:aws:codeguru-security:*:*:scans/CodeWhisperer-*"
      ]
    },
    {
      "Sid" : "sid5",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/CodeWhisperer"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForEC2ScheduledInstances

Beschreibung: Ermöglicht es EC2 geplanten Instances, Spot-Instances zu starten und zu verwalten.

`AWSServiceRoleForEC2ScheduledInstances`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Oktober 2017, 18:31 Uhr UTC
- Zeit bearbeitet: 12. Oktober 2017, 18:31 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForEC2ScheduledInstances`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "aws:ec2sri:scheduledInstanceId"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2sri:scheduledInstanceId" : "*"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy

Beschreibung: AWS GroundStation verwendet diese dienstbezogene Rolle, um öffentliche Adressen aufzurufen EC2 IPv4

`AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Dezember 2022, 23:52 UTC
- Bearbeitete Zeit: 13. Dezember 2022, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForGroundStationDataflowEndpointGroupPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForImageBuilder

Beschreibung: Ermöglicht EC2 ImageBuilder das Anrufen von AWS Diensten in Ihrem Namen.

`AWSServiceRoleForImageBuilder`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 29. November 2019, 22:02 UTC
- Bearbeitete Zeit: 23. Juli 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForImageBuilder`

Version der Richtlinie

Richtlinienversion: v21 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:RegisterImage",
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
```

```
            "ec2.amazonaws.com.cn",
            "vmie.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateLaunchTemplate",
        "ec2:DeregisterImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeImportImageTasks",
        "ec2:DescribeExportImageTasks",
        "ec2:DescribeSnapshots",
        "ec2:DescribeHosts"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute"
      ],
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateImage"
          ],
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:export-image-task/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder",
            "EC2 Fast Launch"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "license-manager:UpdateLicenseSpecificationsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:Publish"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:AddTagsToResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:ListInventoryEntries",
        "ssm:SendAutomationSignal",
        "ssm:DescribeInstanceAssociationsStatus",
        "ssm:DescribeAssociationExecutions",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunPowerShellScript",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWSEC2-RunSysprep",
        "arn:aws:s3:::*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:StartAutomationExecution",
      "Resource" : "arn:aws:ssm:*:*:automation-definition/ImageBuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "kms:EncryptionContextKeys" : [
            "aws:ebs:id"
          ]
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "kms:CreateGrant",
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
```

```
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/EC2ImageBuilderDistributionCrossAccountRole"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:DescribeLaunchTemplates",
        "ec2:ModifyLaunchTemplate",
        "ec2:DescribeLaunchTemplateVersions"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ExportImage"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelExportTask"
      ],
      "Resource" : "arn:aws:ec2:*:*:export-image-task/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ssm.amazonaws.com",
            "ec2fastlaunch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch"
      ],
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "inspector2:ListCoverage",
        "inspector2:ListFindings"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/image-builder-*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/CreatedBy" : "EC2 Image Builder"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/ImageBuilder-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/imagebuilder/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForIoTSiteWise

Beschreibung: Ermöglicht AWS IoT SiteWise die Bereitstellung und Verwaltung von Gateways sowie die Abfrage von Daten. Die Richtlinie umfasst die erforderlichen AWS Greengrass-Berechtigungen für die Bereitstellung in Gruppen, AWS Lambda-Berechtigungen für die Erstellung und Aktualisierung von Funktionen mit Servicepräfix und AWS IoT Analytics Analytics-Berechtigungen für die Abfrage von Daten aus Datenspeichern.

`AWSServiceRoleForIoTSiteWise`AWS ist eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2018, 19:19 UTC
- Bearbeitete Zeit: 13. November 2023, 18:27 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForIoTSiteWise`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AllowSiteWiseReadGreenGrass",
      "Effect" : "Allow",
      "Action" : [
        "greengrass:GetAssociatedRole",
        "greengrass:GetCoreDefinition",
        "greengrass:GetCoreDefinitionVersion",
        "greengrass:GetGroup",
        "greengrass:GetGroupVersion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*"
    },
    {
      "Sid" : "AllowSiteWiseAccessLog",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/iotsitewise*:log-stream:*"
    },
    {
      "Sid" : "AllowSiteWiseAccessSiteWiseManagedWorkspaceInTwinMaker",
      "Effect" : "Allow",
      "Action" : [
        "iottwinmaker:GetWorkspace",
        "iottwinmaker:ExecuteQuery"
      ],
      "Resource" : "arn:aws:iottwinmaker:*:*:workspace/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "iottwinmaker:linkedServices" : [
            "IOTSITEWISE"
          ]
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForLogDeliveryPolicy

Beschreibung: Ermöglicht dem Log Delivery Service, Protokolle zu übermitteln, indem er das Protokollziel in Ihrem Namen anruft.

`AWSServiceRoleForLogDeliveryPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Oktober 2019, 17:31 UTC
- Bearbeitete Zeit: 16. Januar 2025, 21:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForLogDeliveryPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LogDeliveryToFirehose",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:ListTagsForDeliveryStream"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/LogDeliveryEnabled" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForMonitronPolicy

Beschreibung: Erteilt Amazon Monitron Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich der AWS SSO-Benutzerzuweisung in Ihrem Namen.

`AWSServiceRoleForMonitronPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Dezember 2020, 19:06 UTC
- Bearbeitete Zeit: 2. Oktober 2024, 10:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForMonitronPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:GetProfile",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:AssociateProfile",
        "sso:ListDirectoryAssociations",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
```

```
        "sso:CreateApplicationAssignment",
        "sso:ListApplicationAssignments"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForNeptuneGraphPolicy

Beschreibung: Bietet Cloudwatch-Zugriff zur Veröffentlichung von Betriebs- und Nutzungsmetriken und Protokollen für Amazon Neptune

`AWSServiceRoleForNeptuneGraphPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 14:03 UTC
- Bearbeitete Zeit: 29. November 2023, 14:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForNeptuneGraphPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GraphMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Neptune",
            "AWS/Usage"
          ]
        }
      }
    },
    {
      "Sid" : "GraphLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GraphLogEvents",
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForPrivateMarketplaceAdminPolicy

Beschreibung: Bietet Berechtigungen zur Beschreibung und Aktualisierung von Private Marketplace-Ressourcen und zur Beschreibung von AWS Organizations

`AWSServiceRoleForPrivateMarketplaceAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 14. Februar 2024, 22:28 UTC
- Bearbeitete Zeit: 14. Februar 2024, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForPrivateMarketplaceAdminPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PrivateMarketplaceCatalogDescribePermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeEntity"
      ],
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Audience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ProcurementPolicy/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/BrandingSettings/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceCatalogDescribeChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:DescribeChangeSet"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "PrivateMarketplaceCatalogListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ListEntities",
        "aws-marketplace:ListChangeSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateMarketplaceStartChangeSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:StartChangeSet"
      ],
      "Condition" : {
        "StringEquals" : {
          "catalog:ChangeType" : [
            "AssociateAudience",
            "DisassociateAudience"
          ]
        }
      },
      "Resource" : [
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/Experience/*",
        "arn:aws:aws-marketplace:*:*:AWSMarketplace/ChangeSet/*"
      ]
    },
    {
      "Sid" : "PrivateMarketplaceOrganizationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListChildren"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForProcurementInsightsPolicy

Beschreibung: Richtlinie für Procurement Insights zum Abrufen von Kontodetails der Organisation

`AWSServiceRoleForProcurementInsightsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 03. Oktober 2024, 14:26 UTC
- Bearbeitete Zeit: 03. Oktober 2024, 14:26 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForProcurementInsightsPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ProcurementInsightsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForSMS

Beschreibung: Bietet Zugriff auf AWS Dienste und Ressourcen, die für die Migration von Dienstinstanzen in AWS S3 EC2 und Cloudformation erforderlich sind.

`AWSServiceRoleForSMS`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. August 2019, 18:39 Uhr UTC
- Zeit bearbeitet: 15. Oktober 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForSMS`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
```

```
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
```

```
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRoleForUserSubscriptions

Beschreibung: Ermöglicht den Zugriff auf Ihre Identity Center-Ressourcen über den Service Benutzerabonnements, um Ihre Abonnements automatisch zu aktualisieren.

`AWSServiceRoleForUserSubscriptions`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. April 2024, 16:14 UTC
- Bearbeitete Zeit: 29. Oktober 2025, 14:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRoleForUserSubscriptions`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SubscriptionManagementPolicy",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeGroup",
        "identitystore:DescribeUser",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "organizations:DescribeOrganization",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso-directory:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRolePolicyForBackupReports

Beschreibung: Bietet AWS Backup-Berechtigungen zum Erstellen von Compliance-Berichten in Ihrem Namen

`AWSServiceRolePolicyForBackupReports`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. August 2021, 21:16 UTC
- Bearbeitete Zeit: 10. März 2023, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupReports`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeFramework",
        "backup:ListBackupJobs",
        "backup:ListRestoreJobs",
        "backup:ListCopyJobs"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:BatchGetResourceConfig",
        "config:SelectResourceConfig",
        "config:DescribeConfigurationAggregators",
```

```
        "config:SelectAggregateResourceConfig",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "s3:GetBucketLocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/
backup.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigurationAggregator",
        "config:PutConfigurationAggregator"
      ],
      "Resource" : "arn:aws:config:*:*:config-aggregator/aws-service-config-aggregator/
backup.amazonaws.com*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRolePolicyForBackupRestoreTesting

Beschreibung: Diese Richtlinie enthält Berechtigungen zum Testen von Wiederherstellungen und zum Bereinigen von Ressourcen, die während der Tests erstellt wurden.

`AWSServiceRolePolicyForBackupRestoreTesting`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. November 2023, 23:37 UTC
- Bearbeitete Zeit: 14. Februar 2024, 22:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForBackupRestoreTesting`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BackupActions",
      "Effect" : "Allow",
      "Action" : [
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRestoreJob",
        "backup:DescribeProtectedResource",
        "backup:GetRecoveryPointRestoreMetadata",
        "backup:ListBackupVaults",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
```

```
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByResource",
        "backup:ListTags",
        "backup:StartRestoreJob"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "backup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshotTierStatus",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeMountTargets",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeDBClusterAutomatedBackups",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteVolume",
        "ec2:TerminateInstances",
        "elasticfilesystem:DeleteFilesystem",
        "elasticfilesystem:DeleteMountTarget",
        "rds:DeleteDBCluster",
        "rds:DeleteDBInstance",
        "fsx:DeleteFileSystem",
        "fsx:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/awsbackup-restore-test" : "false"
        }
      }
    },
    {
      "Sid" : "DdbDeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDeleteActions",
      "Effect" : "Allow",
      "Action" : "redshift:DeleteCluster",
      "Resource" : "arn:aws:redshift:*:*:cluster:awsbackup-restore-test-*"
    },
    {
      "Sid" : "S3DeleteActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
```

```
      "Resource" : "arn:aws:s3:::awsbackup-restore-test-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TimestreamDeleteActions",
      "Effect" : "Allow",
      "Action" : "timestream:DeleteTable",
      "Resource" : "arn:aws:timestream:*:*:database/*/table/awsbackup-restore-test-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSServiceRolePolicyForWorkspacesInstances

Beschreibung: Diese verwaltete Richtlinie bietet Administratorzugriff auf Amazon WorkSpaces zur Verwaltung von EC2 Instances in Ihrem AWS-Konto

`AWSServiceRolePolicyForWorkspacesInstances`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Juni 2025, 20:37 UTC

- Bearbeitete Zeit: 11. Juni 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSServiceRolePolicyForWorkspacesInstances`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeVolumes"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:DeleteVolume",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ManagedResourceOperator" : "workspaces-instances.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSShieldDRTAccessPolicy

Beschreibung: Bietet dem AWS DDo S Response Team eingeschränkten Zugriff auf Sie, AWS-Konto um Sie bei der Abwehr von DDo S-Angriffen bei einem Ereignis mit hohem Schweregrad zu unterstützen.

`AWSShieldDRTAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSShieldDRTAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 5. Juni 2018, 22:29 Uhr UTC
- Bearbeitete Zeit: 15. Dezember 2020, 17:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSShieldDRTAccessPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SRTAccessProtectedResources",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:List*",
        "route53:List*",
        "elasticloadbalancing:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator",
        "ec2:DescribeRegions",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SRTManageProtections",
      "Effect" : "Allow",
      "Action" : [
        "shield:*",
        "waf:*",
        "wafv2:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "cloudfront:UpdateDistribution",
        "apigateway:SetWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSShieldServiceRolePolicy

Beschreibung: Ermöglicht AWS Shield, in Ihrem Namen auf AWS Ressourcen zuzugreifen, um DDo S-Schutz zu bieten.

`AWSShieldServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2021, 19:17 UTC
- Bearbeitete Zeit: 17. November 2021, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSShieldServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSShield",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACL",
        "wafv2:UpdateWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListResourcesForWebACL",
        "cloudfront:ListDistributions",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSocialMessagingServiceRolePolicy

Beschreibung: Bietet Zugriff auf die Veröffentlichung von Metriken und bietet Einblicke für den Versand Ihrer sozialen Nachrichten.

`AWSSocialMessagingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Oktober 2024, 19:28 UTC
- Bearbeitete Zeit: 10. Oktober 2024, 19:28 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSocialMessagingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudwatchMetricPublishing",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SocialMessaging"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSMForSAPServiceLinkedRolePolicy

Beschreibung: Stellt AWS Systems Manager for SAP die Berechtigungen bereit, die für die Verwaltung und Integration von SAP-Software erforderlich sind AWS.

`AWSSSMForSAPServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. November 2022, 01:18 UTC
- Bearbeitete Zeit: 12. August 2025, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMForSAPServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "DescribeInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVolumes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcs",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeInstanceStatus",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeInstanceStatus",
      "Resource" : "*"
    },
    {
      "Sid" : "TargetRuleActions",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:PutTargets",
        "events:DescribeRule",
        "events:PutRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:*:events:*:*:rule/SSMSAPManagedRule*",
        "arn:*:events:*:*:event-bus/default"
      ]
    },
    {
      "Sid" : "DocumentActions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:SendCommand"
      ],
```

```
      "Resource" : [
        "arn:*:ssm:*:*:document/AWSSystemsManagerSAP-*",
        "arn:*:ssm:*:*:document/AWSSSMSAP*",
        "arn:*:ssm:*:*:document/AWSSAP*"
      ]
    },
    {
      "Sid" : "CustomerSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ssm:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "InstanceTagActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/awsApplication" : "false"
        },
        "StringEqualsIgnoreCase" : {
          "ec2:ResourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "DescribeTag",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeTags",
      "Resource" : "*"
    },
    {
      "Sid" : "GetApplication",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetApplication",
```

```
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "UpdateOrDeleteApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:DeleteApplication",
        "servicecatalog:UpdateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:TagResource",
        "servicecatalog:CreateApplication"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicecatalog-
appregistry.amazonaws.com/AWSServiceRoleForAWSServiceCatalogAppRegistry",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicecatalog-appregistry.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutMetricData",
```

```
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : [
            "AWS/Usage",
            "AWS/SSMForSAP"
          ]
        }
      }
    },
    {
      "Sid" : "CreateAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:CreateAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "GetAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:GetAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*"
    },
    {
      "Sid" : "DeleteAttributeGroup",
      "Effect" : "Allow",
      "Action" : "servicecatalog:DeleteAttributeGroup",
      "Resource" : "arn:*:servicecatalog:*:*:/attribute-groups/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "AttributeGroupActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : "arn:*:servicecatalog:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "ListAssociatedAttributeGroups",
      "Effect" : "Allow",
      "Action" : "servicecatalog:ListAssociatedAttributeGroups",
      "Resource" : "arn:*:servicecatalog:*:*:*"
    },
    {
      "Sid" : "CreateGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "GetGroup",
      "Effect" : "Allow",
      "Action" : "resource-groups:GetGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*"
    },
    {
      "Sid" : "DeleteGroup",
      "Effect" : "Allow",
```

```
      "Action" : "resource-groups:DeleteGroup",
      "Resource" : "arn:*:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPCreated" : "True"
        }
      }
    },
    {
      "Sid" : "CreateAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "TagAppTagResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag"
      ],
      "Resource" : "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableAWSServiceCatalogAppRegistry" : "true"
        }
      }
    },
    {
      "Sid" : "GetAppTagResourceGroupConfig",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupConfiguration"
      ],
      "Resource" : [
        "arn:*:resource-groups:*:*:group/AWS_AppRegistry_AppTag_*"
      ]
    },
```

```
    {
      "Sid" : "StartStopInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource" : "arn:*:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    },
    {
      "Sid" : "SsmSapResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:Tag",
        "resource-groups:CreateGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/SystemsManagerForSAP-*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SSMForSAPCreated" : "True"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SSMForSAPCreated"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEc2Instances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SSMForSAPManaged" : "True"
```

```
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageSsmSapTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "SystemsManagerForSAP-*"
          ]
        }
      }
    },
    {
      "Sid" : "ManageAppTagsOnEbsVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "ArnLike" : {
          "aws:RequestTag/awsApplication" : "arn:aws:resource-groups:*:*:group/*/*"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "awsApplication"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "ManageCostAllocationTags",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:StartCostAllocationTagBackfill"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSMOpsInsightsServiceRolePolicy

Beschreibung: Richtlinie für die Rolle „Service Linked“ AWSServiceRoleForAmazonSSM_OpsInsights

`AWSSSMOpsInsightsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Juni 2021, 20:12 UTC
- Bearbeitete Zeit: 16. Juni 2021, 20:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSMOpsInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem",
        "ssm:AddTagsToResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateOpsItem",
        "ssm:GetOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SsmOperationalInsight" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSODirectoryAdministrator

Beschreibung: Administratorzugriff für das SSO-Verzeichnis

`AWSSSODirectoryAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSSODirectoryAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Oktober 2018, 23:54 UTC
- Bearbeitete Zeit: 16. September 2025, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryAdministrator`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AWSSSODirectoryAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSODirectoryReadOnly

Beschreibung: ReadOnly Zugriff auf das SSO-Verzeichnis

`AWSSSODirectoryReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSSODirectoryReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Oktober 2018, 23:49 UTC
- Bearbeitete Zeit: 16. September 2025, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSODirectoryReadOnly`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSODirectoryReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:Search*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Get*",
        "identitystore:Describe*",
        "identitystore:List*",
        "identitystore-auth:ListSessions",
        "identitystore-auth:BatchGetSession"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOMasterAccountAdministrator

Beschreibung: Bietet Zugriff innerhalb von AWS SSO zur Verwaltung der Master- und Mitgliedskonten von AWS Organizations sowie der Cloud-Anwendung

`AWSSSOMasterAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSSOMasterAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 27. Juni 2018, 20:36 UTC
- Bearbeitete Zeit: 16. September 2025, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMasterAccountAdministrator`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
        }
      }
    },
    {
```

```
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOMemberAccountAdministrator

Beschreibung: Bietet Zugriff innerhalb von AWS SSO zur Verwaltung von Mitgliedskonten und Cloud-Anwendungen von AWS Organizations

`AWSSSOMemberAccountAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSSOMemberAccountAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2018, 20:45 Uhr UTC
- Bearbeitete Zeit: 16. September 2025, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSSOMemberAccountAdministrator`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOMemberAccountAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AWSSSOManageDelegatedAdministrator",
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyUseViaAWSIdentityStoreService",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Encrypt",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" : "*"
```

```
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS SSO-Konfigurationen.

`AWSSSOReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSSOReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2018, 20:24 UTC
- Bearbeitete Zeit: 16. September 2025, 19:49 UTC

- ARN: `arn:aws:iam::aws:policy/AWSSSOReadOnly`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedAdministrators",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso:Search*",
        "sso-directory:DescribeDirectory",
        "access-analyzer:ValidatePolicy",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowKMSKeyUseViaAWSIAMIdentityCenterService",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn" : "*"
        }
      }
    },
    {
      "Sid" : "AllowKMSKeyDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSSOServiceRolePolicy

Beschreibung: Gewährt AWS SSO-Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich IAM-Rollen, Richtlinien und SAML-IdP, in Ihrem Namen.

`AWSSSOServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Dezember 2017, 18:36 Uhr UTC
- Zeit bearbeitet: 11. Februar 2025, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSSOServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v18 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMRoleProvisioningActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:DeleteRolePermissionsBoundary"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMRoleReadActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMRoleCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ]
    },
    {
      "Sid" : "IAMSLRCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCreationAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalOrgMasterAccountId" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMSAMLProviderUpdateAction",
      "Effect" : "Allow",
      "Action" : [
        "iam:UpdateSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Sid" : "IAMSAMLProviderCleanupActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
      ],
      "Resource" : [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
```

```
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowUnauthAppForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:UnauthorizeApplication"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeForDirectory",
      "Effect" : "Allow",
      "Action" : [
        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribeAndListOperationsOnIdentitySource",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDeleteSyncProfile",
```

```
      "Effect" : "Allow",
      "Action" : [
        "identity-sync:DeleteSyncProfile"
      ],
      "Resource" : [
        "arn:aws:identity-sync:*:*:profile/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsConsoleFullAccess

Beschreibung: Eine Zugriffsrichtlinie für den user/role/etc Zugriff auf die AWS StepFunctions Konsole. Für ein vollständiges Konsolenerlebnis benötigt ein Benutzer zusätzlich zu dieser Richtlinie möglicherweise die iam: PassRole -Berechtigung für andere IAM-Rollen, die vom Dienst übernommen werden können.

`AWSStepFunctionsConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSStepFunctionsConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:54 UTC
- Zeit bearbeitet: 12. Januar 2017, 00:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:ListRoles",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/service-role/StatesExecutionRole*"
    },
    {
      "Effect" : "Allow",
      "Action" : "lambda:ListFunctions",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsFullAccess

Beschreibung: Eine Zugriffsrichtlinie für den user/role/etc Zugriff auf die AWS StepFunctions API. Für den Vollzugriff MUSS ein Benutzer zusätzlich zu dieser Richtlinie über die iam: PassRole - Berechtigung für mindestens eine IAM-Rolle verfügen, die vom Dienst übernommen werden kann.

`AWSStepFunctionsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSStepFunctionsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:51 UTC
- Zeit bearbeitet: 11. Januar 2017, 21:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "states:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStepFunctionsReadOnlyAccess

Beschreibung: Eine Zugriffsrichtlinie zur Bereitstellung eines user/role/etc schreibgeschützten Zugriffs auf den AWS StepFunctions Dienst.

`AWSStepFunctionsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSStepFunctionsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Januar 2017, 21:46 Uhr UTC
- Bearbeitete Zeit: 26. April 2024, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStepFunctionsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:ListActivities",
        "states:DescribeStateMachine",
        "states:DescribeStateMachineForExecution",
        "states:ListExecutions",
        "states:DescribeExecution",
        "states:GetExecutionHistory",
        "states:DescribeActivity",
        "states:ListTagsForResource",
        "states:DescribeMapRun",
        "states:ListMapRuns",
        "states:DescribeStateMachineAlias",
        "states:ListStateMachineAliases",
        "states:ListStateMachineVersions",
        "states:ValidateStateMachineDefinition"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Storage Gateway über die AWS-Managementkonsole.

`AWSStorageGatewayFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSStorageGatewayFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. September 2022, 20:26 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "storagegateway:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf AWS Storage Gateway über die AWS-Managementkonsole.

`AWSStorageGatewayReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSStorageGatewayReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 6. September 2022, 20:24 UTC
- ARN: `arn:aws:iam::aws:policy/AWSStorageGatewayReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "fetchStorageGatewayParams",
      "Effect" : "Allow",
      "Action" : "ssm:GetParameters",
```

```
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/storagegateway/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSStorageGatewayServiceRolePolicy

Beschreibung: Dienstbezogene Rolle, die von AWS Storage Gateway verwendet wird, um die Integration anderer AWS Dienste mit Storage Gateway zu ermöglichen.

`AWSStorageGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Februar 2021, 19:03 UTC
- Bearbeitete Zeit: 17. Februar 2021, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSStorageGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "fsx:ListTagsForResource"
      ],
      "Resource" : "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupplyChainFederationAdminAccess

Beschreibung: AWSSupply ChainFederationAdminAccess bietet Verbundbenutzern von AWS Supply Chain Zugriff auf die AWS Supply Chain-Anwendung, einschließlich der erforderlichen Berechtigungen, um Aktionen innerhalb der AWS Supply-Chain-Anwendung auszuführen. Die Richtlinie gewährt Administratorberechtigungen für Benutzer und Gruppen von IAM Identity Center und ist einer Rolle zugeordnet, die von AWS Supply Chain in Ihrem Namen erstellt wurde. Sie sollten keine AWSSupply ChainFederationAdminAccess Richtlinie an andere IAM-Entitäten anhängen.

`AWSSupplyChainFederationAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSupplyChainFederationAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. März 2023, 18:54 UTC
- Bearbeitete Zeit: 30. Oktober 2025, 21:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSSupplyChainFederationAdminAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSupplyChain",
      "Effect" : "Allow",
      "Action" : [
        "scn:*"
      ],
      "Resource" : [
        "arn:aws:scn:*:*:instance/*"
      ]
    },
    {
      "Sid" : "ChimeAppInstance",
      "Effect" : "Allow",
```

```
      "Action" : [
        "chime:BatchCreateChannelMembership",
        "chime:CreateAppInstanceUser",
        "chime:CreateChannel",
        "chime:CreateChannelMembership",
        "chime:CreateChannelModerator",
        "chime:Connect",
        "chime:DeleteChannelMembership",
        "chime:DeleteChannelModerator",
        "chime:DescribeChannelMembershipForAppInstanceUser",
        "chime:GetChannelMembershipPreferences",
        "chime:ListChannelMemberships",
        "chime:ListChannelMembershipsForAppInstanceUser",
        "chime:ListChannelMessages",
        "chime:ListChannelModerators",
        "chime:TagResource",
        "chime:PutChannelMembershipPreferences",
        "chime:SendChannelMessage",
        "chime:UpdateChannelReadMarker",
        "chime:UpdateAppInstanceUser"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/SCNInstanceId" : "*"
        }
      }
    },
    {
      "Sid" : "ChimeChannel",
      "Effect" : "Allow",
      "Action" : [
        "chime:DescribeChannel"
      ],
      "Resource" : [
        "arn:aws:chime:*:*:app-instance/*"
      ]
    },
    {
      "Sid" : "ChimeMessaging",
      "Effect" : "Allow",
      "Action" : [
```

```
        "chime:GetMessagingSessionEndpoint"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "sso:GetManagedApplicationInstance",
        "sso:ListDirectoryAssociations",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:ListProfiles",
        "sso:GetProfile",
        "sso:ListProfileAssociations",
        "sso:ListApplicationAssignments",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:GetApplicationAssignmentConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AppflowConnectorProfile",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateConnectorProfile",
        "appflow:UseConnectorProfile",
        "appflow:DeleteConnectorProfile",
        "appflow:UpdateConnectorProfile"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:connectorprofile/scn-*"
      ]
    },
    {
      "Sid" : "AppflowFlow",
      "Effect" : "Allow",
      "Action" : [
        "appflow:CreateFlow",
        "appflow:DeleteFlow",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:ListFlows",
```

```
        "appflow:StartFlow",
        "appflow:StopFlow",
        "appflow:UpdateFlow",
        "appflow:TagResource",
        "appflow:UntagResource"
      ],
      "Resource" : [
        "arn:aws:appflow:*:*:flow/scn-*"
      ]
    },
    {
      "Sid" : "S3ListAllBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3ListSupplyChainBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ]
    },
    {
      "Sid" : "S3ReadWriteObject",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-supply-chain-data-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "SecretsManagerCreateSecret",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "appflow!*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SecretsManagerPutResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "appflow.amazonaws.com"
          ]
        },
        "StringEqualsIgnoreCase" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "appflow"
        }
      }
    },
    {
      "Sid" : "KMSListKeys",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
```

```
    },
    {
      "Sid" : "KMSListGrants",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "KMSCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "appflow.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringEquals" : {
          "aws:ResourceTag/aws-supply-chain-access" : "true"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAccess

Beschreibung: Ermöglicht Benutzern den Zugriff auf das AWS Support Center.

`AWSSupportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSupportAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 18. Juli 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:*",
        "support-console:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAppFullAccess

Beschreibung: Bietet vollen Zugriff auf die AWS Support App und andere erforderliche Dienste wie AWS Support Service Quotas. Diese Richtlinie beinhaltet Berechtigungen zur Nutzung der unterstützenden Dienste, sodass sich der Benutzer bei AWS Support Supportanfragen an sie wenden, Servicekontingente ändern und die entsprechenden dienstbezogenen Rollen erstellen kann.

`AWSSupportAppFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSupportAppFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2022, 16:53 UTC
- Bearbeitete Zeit: 22. August 2022, 16:53 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:RequestServiceQuotaIncrease",
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeCases",
        "support:DescribeCommunications",
        "support:DescribeSeverityLevels",
        "support:InitiateChatForCase",
        "support:ResolveCase"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportAppReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf die AWS Support App.

`AWSSupportAppReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSupportAppReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. August 2022, 17:01 UTC
- Bearbeitete Zeit: 22. August 2022, 17:01 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportAppReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "support:DescribeCases",
        "support:DescribeCommunications"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportPlansFullAccess

Beschreibung: Bietet vollen Zugriff auf Supportpläne.

`AWSSupportPlansFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSupportPlansFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. September 2022, 18:19 UTC
- Bearbeitete Zeit: 09. September 2024, 21:15 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "supportplans:StartSupportPlanUpdate",
        "supportplans:CreateSupportPlanSchedule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportPlansReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Supportpläne.

`AWSSupportPlansReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `AWSSupportPlansReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. September 2022, 18:08 UTC
- Bearbeitete Zeit: 09. September 2024, 21:21 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSupportPlansReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSupportServiceRolePolicy

Beschreibung: Ermöglicht AWS Support den Zugriff auf AWS Ressourcen zur Bereitstellung von Abrechnungs-, Verwaltungs- und Supportdiensten.

`AWSSupportServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. April 2018, 18:04 UTC
- Bearbeitete Zeit: 8. Dezember 2025, 23:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSupportServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v43 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Statement" : [
    {
      "Sid" : "AWSSupportAPIGatewayAccess",
```

```
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/account",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses",
        "arn:aws:apigateway:*::/apis/*/integrations/*/integrationresponses/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses",
        "arn:aws:apigateway:*::/apis/*/routes/*/routeresponses/*",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/domainnames/*/apimappings/*",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models/*/default_template",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
```

```
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration/responses/
*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/responses/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*/sdks/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/usageplans",
        "arn:aws:apigateway:*::/usageplans/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AWSSupportDeleteRoleAccess",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/support.amazonaws.com/
AWSServiceRoleForSupport"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup1",
      "Action" : [
        "access-analyzer:getAccessPreview",
        "access-analyzer:getAnalyzedResource",
        "access-analyzer:getAnalyzer",
        "access-analyzer:getArchiveRule",
        "access-analyzer:getFinding",
        "access-analyzer:getGeneratedPolicy",
        "access-analyzer:listAccessPreviewFindings",
        "access-analyzer:listAccessPreviews",
        "access-analyzer:listAnalyzedResources",
        "access-analyzer:listAnalyzers",
        "access-analyzer:listArchiveRules",
        "access-analyzer:listFindings",
        "access-analyzer:listPolicyGenerations",
        "account:getRegionOptStatus",
        "account:listRegions",
        "acm-pca:describeCertificateAuthority",
```

```
        "acm-pca:describeCertificateAuthorityAuditReport",
        "acm-pca:getCertificate",
        "acm-pca:getCertificateAuthorityCertificate",
        "acm-pca:getCertificateAuthorityCsr",
        "acm-pca:listCertificateAuthorities",
        "acm-pca:listTags",
        "acm:describeCertificate",
        "acm:getAccountConfiguration",
        "acm:getCertificate",
        "acm:listCertificates",
        "acm:listTagsForCertificate",
        "aiops:getInvestigationGroup",
        "aiops:getInvestigationGroupPolicy",
        "aiops:listInvestigationGroups",
        "airflow:getEnvironment",
        "airflow:listEnvironments",
        "airflow:listTagsForResource",
        "amplify:getApp",
        "amplify:getBackendEnvironment",
        "amplify:getBranch",
        "amplify:getDomainAssociation",
        "amplify:getJob",
        "amplify:getWebhook",
        "amplify:listApps",
        "amplify:listBackendEnvironments",
        "amplify:listBranches",
        "amplify:listDomainAssociations",
        "amplify:listJobs",
        "amplify:listWebhooks",
        "amplifyuibuilder:exportComponents",
        "amplifyuibuilder:exportThemes",
        "aoss:batchGetCollection",
        "aoss:batchGetEffectiveLifecyclePolicy",
        "aoss:batchGetLifecyclePolicy",
        "aoss:batchGetVpcEndpoint",
        "aoss:getAccessPolicy",
        "aoss:getAccountSettings",
        "aoss:getPoliciesStats",
        "aoss:getSecurityConfig",
        "aoss:getSecurityPolicy",
        "aoss:listAccessPolicies",
        "aoss:listCollections",
        "aoss:listLifecyclePolicies",
        "aoss:listSecurityConfigs",
```

```
        "aoss:listSecurityPolicies",
        "aoss:listTagsForResource",
        "aoss:listVpcEndpoints",
        "appconfig:getApplication",
        "appconfig:getConfigurationProfile",
        "appconfig:getDeployment",
        "appconfig:getDeploymentStrategy",
        "appconfig:getEnvironment",
        "appconfig:getExtension",
        "appconfig:getExtensionAssociation",
        "appconfig:listApplications",
        "appconfig:listConfigurationProfiles",
        "appconfig:listDeployments",
        "appconfig:listDeploymentStrategies",
        "appconfig:listEnvironments",
        "appconfig:listExtensionAssociations",
        "appconfig:listExtensions",
        "appconfig:listHostedConfigurationVersions",
        "appflow:describeConnectorEntity",
        "appflow:describeConnectorProfiles",
        "appflow:describeConnectors",
        "appflow:describeFlow",
        "appflow:describeFlowExecutionRecords",
        "appflow:listConnectorEntities",
        "appflow:listFlows",
        "application-autoscaling:describeScalableTargets",
        "application-autoscaling:describeScalingActivities",
        "application-autoscaling:describeScalingPolicies",
        "application-autoscaling:describeScheduledActions",
        "application-signals:getService",
        "application-signals:getServiceLevelObjective",
        "application-signals:listServiceDependencies",
        "application-signals:listServiceDependents",
        "application-signals:listServiceLevelObjectives",
        "application-signals:listServiceOperations",
        "application-signals:listServices",
        "applicationinsights:describeApplication",
        "applicationinsights:describeComponent",
        "applicationinsights:describeComponentConfiguration",
        "applicationinsights:describeComponentConfigurationRecommendation",
        "applicationinsights:describeLogPattern",
        "applicationinsights:describeObservation",
        "applicationinsights:describeProblem",
        "applicationinsights:describeProblemObservations",
```

```
        "applicationinsights:listApplications",
        "applicationinsights:listComponents",
        "applicationinsights:listConfigurationHistory",
        "applicationinsights:listLogPatterns",
        "applicationinsights:listLogPatternSets",
        "applicationinsights:listProblems",
        "appmesh:describeGatewayRoute",
        "appmesh:describeMesh",
        "appmesh:describeRoute",
        "appmesh:describeVirtualGateway",
        "appmesh:describeVirtualNode",
        "appmesh:describeVirtualRouter",
        "appmesh:describeVirtualService",
        "appmesh:listGatewayRoutes",
        "appmesh:listMeshes",
        "appmesh:listRoutes",
        "appmesh:listTagsForResource",
        "appmesh:listVirtualGateways",
        "appmesh:listVirtualNodes",
        "appmesh:listVirtualRouters",
        "appmesh:listVirtualServices",
        "apprunner:describeAutoScalingConfiguration",
        "apprunner:describeCustomDomains",
        "apprunner:describeObservabilityConfiguration",
        "apprunner:describeOperation",
        "apprunner:describeService",
        "apprunner:describeVpcConnector",
        "apprunner:describeVpcIngressConnection",
        "apprunner:listAutoScalingConfigurations",
        "apprunner:listConnections",
        "apprunner:listObservabilityConfigurations",
        "apprunner:listOperations",
        "apprunner:listServices",
        "apprunner:listTagsForResource",
        "apprunner:listVpcConnectors",
        "apprunner:listVpcIngressConnections",
        "appstream:describeAppBlockBuilderAppBlockAssociations",
        "appstream:describeAppBlockBuilders",
        "appstream:describeAppBlocks",
        "appstream:describeApplicationFleetAssociations",
        "appstream:describeApplications",
        "appstream:describeDirectoryConfigs",
        "appstream:describeEntitlements",
        "appstream:describeFleets",
```

```
        "appstream:describeImageBuilders",
        "appstream:describeImagePermissions",
        "appstream:describeImages",
        "appstream:describeSessions",
        "appstream:describeStacks",
        "appstream:describeUsageReportSubscriptions",
        "appstream:describeUsers",
        "appstream:describeUserStackAssociations",
        "appstream:listAssociatedFleets",
        "appstream:listAssociatedStacks",
        "appstream:listEntitledApplications",
        "appstream:listTagsForResource",
        "appsync:evaluateCode",
        "appsync:evaluateMappingTemplate",
        "appsync:getApi",
        "appsync:getApiAssociation",
        "appsync:getApiCache",
        "appsync:getChannelNamespace",
        "appsync:getDataSource",
        "appsync:getDataSourceIntrospection",
        "appsync:getDomainName",
        "appsync:getFunction",
        "appsync:getGraphqlApi",
        "appsync:getGraphqlApiEnvironmentVariables",
        "appsync:getIntrospectionSchema",
        "appsync:getResolver",
        "appsync:getSchemaCreationStatus",
        "appsync:getSourceApiAssociation",
        "appsync:getType",
        "appsync:listApis",
        "appsync:listChannelNamespaces",
        "appsync:listDataSources",
        "appsync:listDomainNames",
        "appsync:listFunctions",
        "appsync:listGraphqlApis",
        "appsync:listResolvers",
        "appsync:listResolversByFunction",
        "appsync:listSourceApiAssociations",
        "appsync:listTypes",
        "appsync:listTypesByAssociation",
        "aps:describeAlertManagerDefinition",
        "aps:describeRuleGroupsNamespace",
        "aps:describeScraper",
        "aps:describeWorkspace",
```

```
        "aps:listRuleGroupsNamespaces",
        "aps:listScrapers",
        "aps:listWorkspaces",
        "athena:batchGetNamedQuery",
        "athena:batchGetQueryExecution",
        "athena:getCalculationExecution",
        "athena:getCalculationExecutionStatus",
        "athena:getCapacityAssignmentConfiguration",
        "athena:getCapacityReservation",
        "athena:getDataCatalog",
        "athena:getNamedQuery",
        "athena:getNotebookMetadata",
        "athena:getQueryExecution",
        "athena:getQueryRuntimeStatistics",
        "athena:getSession",
        "athena:getSessionStatus",
        "athena:getWorkGroup",
        "athena:listApplicationDPUSizes",
        "athena:listCalculationExecutions",
        "athena:listCapacityReservations",
        "athena:listDataCatalogs",
        "athena:listEngineVersions",
        "athena:listExecutors",
        "athena:listNamedQueries",
        "athena:listNotebookMetadata",
        "athena:listNotebookSessions",
        "athena:listQueryExecutions",
        "athena:listSessions",
        "athena:listTagsForResource",
        "athena:listWorkGroups",
        "auditmanager:getAccountStatus",
        "auditmanager:getDelegations",
        "auditmanager:listAssessmentFrameworks",
        "auditmanager:listAssessmentReports",
        "auditmanager:listAssessments",
        "auditmanager:listControls",
        "auditmanager:listKeywordsForDataSource",
        "auditmanager:listNotifications",
        "autoscaling-plans:describeScalingPlanResources",
        "autoscaling-plans:describeScalingPlans",
        "autoscaling-plans:getScalingPlanResourceForecastData",
        "autoscaling:describeAccountLimits",
        "autoscaling:describeAdjustmentTypes",
        "autoscaling:describeAutoScalingGroups",
```

```
        "autoscaling:describeAutoScalingInstances",
        "autoscaling:describeAutoScalingNotificationTypes",
        "autoscaling:describeInstanceRefreshes",
        "autoscaling:describeLaunchConfigurations",
        "autoscaling:describeLifecycleHooks",
        "autoscaling:describeLifecycleHookTypes",
        "autoscaling:describeLoadBalancers",
        "autoscaling:describeLoadBalancerTargetGroups",
        "autoscaling:describeMetricCollectionTypes",
        "autoscaling:describeNotificationConfigurations",
        "autoscaling:describePolicies",
        "autoscaling:describeScalingActivities",
        "autoscaling:describeScalingProcessTypes",
        "autoscaling:describeScheduledActions",
        "autoscaling:describeTags",
        "autoscaling:describeTerminationPolicyTypes",
        "autoscaling:describeTrafficSources",
        "autoscaling:describeWarmPool",
        "backup-gateway:getBandwidthRateLimitSchedule",
        "backup-gateway:getGateway",
        "backup-gateway:getHypervisor",
        "backup-gateway:getHypervisorPropertyMappings",
        "backup-gateway:getVirtualMachine",
        "backup-gateway:listGateways",
        "backup-gateway:listHypervisors",
        "backup-gateway:listVirtualMachines",
        "backup-search:listSearchJobBackups",
        "backup-search:listSearchJobs",
        "backup:describeBackupJob",
        "backup:describeBackupVault",
        "backup:describeCopyJob",
        "backup:describeFramework",
        "backup:describeGlobalSettings",
        "backup:describeProtectedResource",
        "backup:describeRecoveryPoint",
        "backup:describeRegionSettings",
        "backup:describeReportJob",
        "backup:describeReportPlan",
        "backup:describeRestoreJob",
        "backup:getBackupPlan",
        "backup:getBackupPlanFromJSON",
        "backup:getBackupPlanFromTemplate",
        "backup:getBackupSelection",
        "backup:getBackupVaultAccessPolicy",
```

```
        "backup:getBackupVaultNotifications",
        "backup:getLegalHold",
        "backup:getRecoveryPointRestoreMetadata",
        "backup:getRecoveryPointIndexDetails",
        "backup:getRestoreJobMetadata",
        "backup:getRestoreTestingInferredMetadata",
        "backup:getRestoreTestingPlan",
        "backup:getRestoreTestingSelection",
        "backup:getSupportedResourceTypes",
        "backup:listBackupJobs",
        "backup:listBackupPlans",
        "backup:listBackupPlanTemplates",
        "backup:listBackupPlanVersions",
        "backup:listBackupSelections",
        "backup:listBackupVaults",
        "backup:listCopyJobs",
        "backup:listFrameworks",
        "backup:listIndexedRecoveryPoints",
        "backup:listLegalHolds",
        "backup:listProtectedResources",
        "backup:listRecoveryPointsByBackupVault",
        "backup:listRecoveryPointsByLegalHold",
        "backup:listRecoveryPointsByResource",
        "backup:listReportJobs",
        "backup:listReportPlans",
        "backup:listRestoreJobs",
        "backup:listRestoreJobsByProtectedResource",
        "backup:listRestoreTestingPlans",
        "backup:listRestoreTestingSelections",
        "backup:listTags",
        "batch:describeComputeEnvironments",
        "batch:describeJobDefinitions",
        "batch:describeJobQueues",
        "batch:describeJobs",
        "batch:describeSchedulingPolicies",
        "batch:listJobs",
        "bedrock:getAgent",
        "bedrock:getAgentActionGroup",
        "bedrock:getAgentAlias",
        "bedrock:getAgentKnowledgeBase",
        "bedrock:getAgentVersion",
        "bedrock:getCustomModel",
        "bedrock:getDataSource",
        "bedrock:getEvaluationJob",
```

```
        "bedrock:getFlow",
        "bedrock:getFlowAlias",
        "bedrock:getFlowVersion",
        "bedrock:getFoundationModel",
        "bedrock:getGuardrail",
        "bedrock:getImportedModel",
        "bedrock:getInferenceProfile",
        "bedrock:getIngestionJob",
        "bedrock:getKnowledgeBase",
        "bedrock:getMarketplaceModelEndpoint",
        "bedrock:getModelCopyJob",
        "bedrock:getModelCustomizationJob",
        "bedrock:getModelImportJob",
        "bedrock:getModelInvocationJob",
        "bedrock:getModelInvocationLoggingConfiguration",
        "bedrock:getPrompt",
        "bedrock:getPromptRouter",
        "bedrock:getProvisionedModelThroughput",
        "bedrock:listAgentActionGroups",
        "bedrock:listAgentAliases",
        "bedrock:listAgentKnowledgeBases",
        "bedrock:listAgents",
        "bedrock:listAgentVersions",
        "bedrock:listCustomModels",
        "bedrock:listDataSources",
        "bedrock:listEvaluationJobs",
        "bedrock:listFlowAliases",
        "bedrock:listFlows",
        "bedrock:listFlowVersions",
        "bedrock:listFoundationModels",
        "bedrock:listGuardrails",
        "bedrock:listImportedModels",
        "bedrock:listInferenceProfiles",
        "bedrock:listIngestionJobs",
        "bedrock:listKnowledgeBases",
        "bedrock:listMarketplaceModelEndpoints",
        "bedrock:listModelCopyJobs",
        "bedrock:listModelCustomizationJobs",
        "bedrock:listModelImportJobs",
        "bedrock:listModelInvocationJobs",
        "bedrock:listPromptRouters",
        "bedrock:listPrompts",
        "bedrock:listProvisionedModelThroughputs",
        "braket:getDevice",
```

```
        "braket:getQuantumTask",
        "braket:searchDevices",
        "braket:searchQuantumTasks",
        "budgets:viewBudget",
        "ce:getCostAndUsage",
        "ce:getCostAndUsageWithResources",
        "ce:getCostForecast",
        "ce:getDimensionValues",
        "ce:getReservationCoverage",
        "ce:getReservationPurchaseRecommendation",
        "ce:getReservationUtilization",
        "ce:getRightsizingRecommendation",
        "ce:getSavingsPlansCoverage",
        "ce:getSavingsPlansPurchaseRecommendation",
        "ce:getSavingsPlansUtilization",
        "ce:getSavingsPlansUtilizationDetails",
        "ce:getTags",
        "chime:describeAppInstance",
        "chime:getAttendee",
        "chime:getGlobalSettings",
        "chime:getMediaCapturePipeline",
        "chime:getMediaPipeline",
        "chime:getMeeting",
        "chime:getProxySession",
        "chime:getSipMediaApplication",
        "chime:getSipRule",
        "chime:getVoiceConnector",
        "chime:getVoiceConnectorGroup",
        "chime:getVoiceConnectorLoggingConfiguration",
        "chime:listAppInstances",
        "chime:listAttendees",
        "chime:listChannelBans",
        "chime:listChannels",
        "chime:listChannelsModeratedByAppInstanceUser",
        "chime:listMediaCapturePipelines",
        "chime:listMediaPipelines",
        "chime:listMeetings",
        "chime:listSipMediaApplications",
        "chime:listSipRules",
        "chime:listVoiceConnectorGroups",
        "chime:listVoiceConnectors",
        "cleanrooms:batchGetCollaborationAnalysisTemplate",
        "cleanrooms:batchGetSchema",
        "cleanrooms:getAnalysisTemplate",
```

```
        "cleanrooms:getCollaboration",
        "cleanrooms:getCollaborationAnalysisTemplate",
        "cleanrooms:getCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:getCollaborationPrivacyBudgetTemplate",
        "cleanrooms:getConfiguredTable",
        "cleanrooms:getConfiguredTableAnalysisRule",
        "cleanrooms:getConfiguredTableAssociation",
        "cleanrooms:getConfiguredAudienceModelAssociation",
        "cleanrooms:getMembership",
        "cleanrooms:getPrivacyBudgetTemplate",
        "cleanrooms:getSchema",
        "cleanrooms:getSchemaAnalysisRule",
        "cleanrooms:listAnalysisTemplates",
        "cleanrooms:listCollaborationAnalysisTemplates",
        "cleanrooms:listCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:listCollaborationPrivacyBudgetTemplates",
        "cleanrooms:listCollaborationPrivacyBudgets",
        "cleanrooms:listCollaborations",
        "cleanrooms:listConfiguredAudienceModelAssociations",
        "cleanrooms:listConfiguredTableAssociations",
        "cleanrooms:listConfiguredTables",
        "cleanrooms:listMembers",
        "cleanrooms:listMemberships",
        "cleanrooms:listPrivacyBudgetTemplates",
        "cleanrooms:listPrivacyBudgets",
        "cleanrooms:listProtectedQueries",
        "cleanrooms:listSchemas",
        "cleanrooms:previewPrivacyImpact",
        "cloud9:describeEnvironmentMemberships",
        "cloud9:describeEnvironments",
        "cloud9:listEnvironments",
        "clouddirectory:getDirectory",
        "clouddirectory:listDirectories",
        "cloudformation:batchDescribeTypeConfigurations",
        "cloudformation:describeAccountLimits",
        "cloudformation:describeChangeSet",
        "cloudformation:describeChangeSetHooks",
        "cloudformation:describePublisher",
        "cloudformation:describeStackDriftDetectionStatus",
        "cloudformation:describeStackEvents",
        "cloudformation:describeStackInstance",
        "cloudformation:describeStackResource",
        "cloudformation:describeStackResourceDrifts",
        "cloudformation:describeStackResources",
```

```
        "cloudformation:describeStacks",
        "cloudformation:describeStackSet",
        "cloudformation:describeStackSetOperation",
        "cloudformation:describeType",
        "cloudformation:describeTypeRegistration",
        "cloudformation:estimateTemplateCost",
        "cloudformation:getResource",
        "cloudformation:getStackPolicy",
        "cloudformation:getTemplate",
        "cloudformation:getTemplateSummary",
        "cloudformation:listChangeSets",
        "cloudformation:listExports",
        "cloudformation:listImports",
        "cloudformation:listResources",
        "cloudformation:listStackInstances",
        "cloudformation:listStackResources",
        "cloudformation:listStacks",
        "cloudformation:listStackSetOperationResults",
        "cloudformation:listStackSetOperations",
        "cloudformation:listStackSets",
        "cloudformation:listTypeRegistrations",
        "cloudformation:listTypes",
        "cloudformation:listTypeVersions",
        "cloudfront:describeFunction",
        "cloudfront:describeKeyValueStore",
        "cloudfront:getAnycastIpList",
        "cloudfront:getCachePolicy",
        "cloudfront:getCachePolicyConfig",
        "cloudfront:getCloudFrontOriginAccessIdentity",
        "cloudfront:getCloudFrontOriginAccessIdentityConfig",
        "cloudfront:getContinuousDeploymentPolicy",
        "cloudfront:getContinuousDeploymentPolicyConfig",
        "cloudfront:getDistribution",
        "cloudfront:getDistributionConfig",
        "cloudfront:getInvalidation",
        "cloudfront:getKeyGroup",
        "cloudfront:getKeyGroupConfig",
        "cloudfront:getMonitoringSubscription",
        "cloudfront:getOriginAccessControl",
        "cloudfront:getOriginAccessControlConfig",
        "cloudfront:getOriginRequestPolicy",
        "cloudfront:getOriginRequestPolicyConfig",
        "cloudfront:getPublicKey",
        "cloudfront:getPublicKeyConfig",
```

```
        "cloudfront:getRealtimeLogConfig",
        "cloudfront:getResponseHeadersPolicy",
        "cloudfront:getResponseHeadersPolicyConfig",
        "cloudfront:getStreamingDistribution",
        "cloudfront:getStreamingDistributionConfig",
        "cloudfront:getVpcOrigin",
        "cloudfront:listAnycastIpLists",
        "cloudfront:listCachePolicies",
        "cloudfront:listCloudFrontOriginAccessIdentities",
        "cloudfront:listConflictingAliases",
        "cloudfront:listContinuousDeploymentPolicies",
        "cloudfront:listDistributions",
        "cloudfront:listDistributionsByAnycastIpListId",
        "cloudfront:listDistributionsByCachePolicyId",
        "cloudfront:listDistributionsByKeyGroup",
        "cloudfront:listDistributionsByOriginRequestPolicyId",
        "cloudfront:listDistributionsByRealtimeLogConfig",
        "cloudfront:listDistributionsByResponseHeadersPolicyId",
        "cloudfront:listDistributionsByVpcOriginId",
        "cloudfront:listDistributionsByWebACLId",
        "cloudfront:listFunctions",
        "cloudfront:listInvalidations",
        "cloudfront:listKeyGroups",
        "cloudfront:listKeyValueStores",
        "cloudfront:listOriginAccessControls",
        "cloudfront:listOriginRequestPolicies",
        "cloudfront:listPublicKeys",
        "cloudfront:listRealtimeLogConfigs",
        "cloudfront:listResponseHeadersPolicies",
        "cloudfront:listStreamingDistributions",
        "cloudfront:listVpcOrigins",
        "cloudhsm:describeBackups",
        "cloudhsm:describeClusters",
        "cloudsearch:describeAnalysisSchemes",
        "cloudsearch:describeAvailabilityOptions",
        "cloudsearch:describeDomains",
        "cloudsearch:describeExpressions",
        "cloudsearch:describeIndexFields",
        "cloudsearch:describeScalingParameters",
        "cloudsearch:describeServiceAccessPolicies",
        "cloudsearch:describeSuggesters",
        "cloudsearch:listDomainNames",
        "cloudtrail:describeTrails",
        "cloudtrail:getEventSelectors",
```

```
        "cloudtrail:getInsightSelectors",
        "cloudtrail:getTrail",
        "cloudtrail:getTrailStatus",
        "cloudtrail:listPublicKeys",
        "cloudtrail:listTags",
        "cloudtrail:listTrails",
        "cloudtrail:lookupEvents",
        "cloudwatch:describeAlarmHistory",
        "cloudwatch:describeAlarms",
        "cloudwatch:describeAlarmsForMetric",
        "cloudwatch:describeAnomalyDetectors",
        "cloudwatch:describeInsightRules",
        "cloudwatch:getDashboard",
        "cloudwatch:getInsightRuleReport",
        "cloudwatch:getMetricData",
        "cloudwatch:getMetricStatistics",
        "cloudwatch:getMetricStream",
        "cloudWatch:getMetricWidgetImage",
        "cloudwatch:listDashboards",
        "cloudwatch:listManagedInsightRules",
        "cloudwatch:listMetrics",
        "cloudwatch:listMetricStreams",
        "codeartifact:describeDomain",
        "codeartifact:describePackageVersion",
        "codeartifact:describeRepository",
        "codeartifact:getDomainPermissionsPolicy",
        "codeartifact:getRepositoryEndpoint",
        "codeartifact:getRepositoryPermissionsPolicy",
        "codeartifact:listDomains",
        "codeartifact:listPackages",
        "codeartifact:listPackageVersionAssets",
        "codeartifact:listPackageVersions",
        "codeartifact:listRepositories",
        "codeartifact:listRepositoriesInDomain",
        "codebuild:batchGetBuildBatches",
        "codebuild:batchGetBuilds",
        "codebuild:batchGetFleets",
        "codebuild:batchGetProjects",
        "codebuild:listBuildBatches",
        "codebuild:listBuildBatchesForProject",
        "codebuild:listBuilds",
        "codebuild:listBuildsForProject",
        "codebuild:listCuratedEnvironmentImages",
        "codebuild:listFleets",
```

```
        "codebuild:listProjects",
        "codebuild:listSourceCredentials",
        "codecommit:batchGetRepositories",
        "codecommit:getBranch",
        "codecommit:getRepository",
        "codecommit:getRepositoryTriggers",
        "codecommit:listBranches",
        "codecommit:listRepositories",
        "codeconnections:getConnection",
        "codeconnections:getHost",
        "codeconnections:getRepositoryLink",
        "codeconnections:getRepositorySyncStatus",
        "codeconnections:getResourceSyncStatus",
        "codeconnections:getSyncBlockerSummary",
        "codeconnections:getSyncConfiguration",
        "codeconnections:listConnections",
        "codeconnections:listHosts",
        "codeconnections:listRepositoryLinks",
        "codeconnections:listRepositorySyncDefinitions",
        "codeconnections:listSyncConfigurations",
        "codedeploy:batchGetApplicationRevisions",
        "codedeploy:batchGetApplications",
        "codedeploy:batchGetDeploymentGroups",
        "codedeploy:batchGetDeploymentInstances",
        "codedeploy:batchGetDeployments",
        "codedeploy:batchGetDeploymentTargets",
        "codedeploy:batchGetOnPremisesInstances",
        "codedeploy:getApplication",
        "codedeploy:getApplicationRevision",
        "codedeploy:getDeployment",
        "codedeploy:getDeploymentConfig",
        "codedeploy:getDeploymentGroup",
        "codedeploy:getDeploymentInstance",
        "codedeploy:getDeploymentTarget",
        "codedeploy:getOnPremisesInstance",
        "codedeploy:listApplicationRevisions",
        "codedeploy:listApplications",
        "codedeploy:listDeploymentConfigs",
        "codedeploy:listDeploymentGroups",
        "codedeploy:listDeploymentInstances",
        "codedeploy:listDeployments",
        "codedeploy:listDeploymentTargets",
        "codedeploy:listGitHubAccountTokenNames",
        "codedeploy:listOnPremisesInstances",
```

```
        "codepipeline:getJobDetails",
        "codepipeline:getPipeline",
        "codepipeline:getPipelineExecution",
        "codepipeline:getPipelineState",
        "codepipeline:listActionExecutions",
        "codepipeline:listActionTypes",
        "codepipeline:listPipelineExecutions",
        "codepipeline:listPipelines",
        "codepipeline:listRuleExecutions",
        "codepipeline:listWebhooks",
        "codestar-connections:getConnection",
        "codestar-connections:getHost",
        "codestar-connections:listConnections",
        "codestar-connections:listHosts",
        "codestar:describeProject",
        "codestar:listProjects",
        "codestar:listResources",
        "codestar:listTeamMembers",
        "codestar:listUserProfiles",
        "cognito-identity:describeIdentity",
        "cognito-identity:describeIdentityPool",
        "cognito-identity:getIdentityPoolAnalytics",
        "cognito-identity:getIdentityPoolDailyAnalytics",
        "cognito-identity:getIdentityPoolRoles",
        "cognito-identity:getIdentityProviderDailyAnalytics",
        "cognito-identity:listIdentities",
        "cognito-identity:listIdentityPools",
        "cognito-identity:lookupDeveloperIdentity",
        "cognito-idp:describeIdentityProvider",
        "cognito-idp:describeResourceServer",
        "cognito-idp:describeRiskConfiguration",
        "cognito-idp:describeUserImportJob",
        "cognito-idp:describeUserPool",
        "cognito-idp:describeUserPoolClient",
        "cognito-idp:describeUserPoolDomain",
        "cognito-idp:getCSVHeader",
        "cognito-idp:getGroup",
        "cognito-idp:getLogDeliveryConfiguration",
        "cognito-idp:getUICustomization",
        "cognito-idp:getUserPoolMfaConfig",
        "cognito-idp:listGroups",
        "cognito-idp:listIdentityProviders",
        "cognito-idp:listResourceServers",
        "cognito-idp:listUserImportJobs",
```

```
        "cognito-idp:listUserPoolClients",
        "cognito-idp:listUserPools",
        "cognito-sync:describeDataset",
        "cognito-sync:describeIdentityPoolUsage",
        "cognito-sync:describeIdentityUsage",
        "cognito-sync:getCognitoEvents",
        "cognito-sync:getIdentityPoolConfiguration",
        "cognito-sync:listDatasets",
        "cognito-sync:listIdentityPoolUsage",
        "comprehend:describeDocumentClassificationJob",
        "comprehend:describeDocumentClassifier",
        "comprehend:describeDominantLanguageDetectionJob",
        "comprehend:describeEndpoint",
        "comprehend:describeEntitiesDetectionJob",
        "comprehend:describeEntityRecognizer",
        "comprehend:describeEventsDetectionJob",
        "comprehend:describeFlywheel",
        "comprehend:describeFlywheelIteration",
        "comprehend:describeKeyPhrasesDetectionJob",
        "comprehend:describePiiEntitiesDetectionJob",
        "comprehend:describeSentimentDetectionJob",
        "comprehend:describeTargetedSentimentDetectionJob",
        "comprehend:describeTopicsDetectionJob",
        "comprehend:listDocumentClassificationJobs",
        "comprehend:listDocumentClassifiers",
        "comprehend:listDominantLanguageDetectionJobs",
        "comprehend:listEndpoints",
        "comprehend:listEntitiesDetectionJobs",
        "comprehend:listEntityRecognizers",
        "comprehend:listEventsDetectionJobs",
        "comprehend:listFlywheelIterationHistory",
        "comprehend:listFlywheels",
        "comprehend:listKeyPhrasesDetectionJobs",
        "comprehend:listPiiEntitiesDetectionJobs",
        "comprehend:listSentimentDetectionJobs",
        "comprehend:listTargetedSentimentDetectionJobs",
        "comprehend:listTopicsDetectionJobs",
        "compute-optimizer:getAutoScalingGroupRecommendations",
        "compute-optimizer:getEBSVolumeRecommendations",
        "compute-optimizer:getEC2InstanceRecommendations",
        "compute-optimizer:getEC2RecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:getECSServiceRecommendations",
        "compute-optimizer:getEnrollmentStatus",
```

```
        "compute-optimizer:getIdleRecommendations",
        "compute-optimizer:getRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:getRDSDatabaseRecommendations",
        "compute-optimizer:getRecommendationSummaries",
        "config:batchGetAggregateResourceConfig",
        "config:batchGetResourceConfig",
        "config:describeAggregateComplianceByConfigRules",
        "config:describeAggregationAuthorizations",
        "config:describeComplianceByConfigRule",
        "config:describeComplianceByResource",
        "config:describeConfigRuleEvaluationStatus",
        "config:describeConfigRules",
        "config:describeConfigurationAggregators",
        "config:describeConfigurationAggregatorSourcesStatus",
        "config:describeConfigurationRecorders",
        "config:describeConfigurationRecorderStatus",
        "config:describeConformancePackCompliance",
        "config:describeConformancePacks",
        "config:describeConformancePackStatus",
        "config:describeDeliveryChannels",
        "config:describeDeliveryChannelStatus",
        "config:describeOrganizationConfigRules",
        "config:describeOrganizationConfigRuleStatuses",
        "config:describeOrganizationConformancePacks",
        "config:describeOrganizationConformancePackStatuses",
        "config:describePendingAggregationRequests",
        "config:describeRemediationConfigurations",
        "config:describeRemediationExceptions",
        "config:describeRemediationExecutionStatus",
        "config:describeRetentionConfigurations",
        "config:getAggregateComplianceDetailsByConfigRule",
        "config:getAggregateConfigRuleComplianceSummary",
        "config:getAggregateDiscoveredResourceCounts",
        "config:getAggregateResourceConfig",
        "config:getComplianceDetailsByConfigRule",
        "config:getComplianceDetailsByResource",
        "config:getComplianceSummaryByConfigRule",
        "config:getComplianceSummaryByResourceType",
        "config:getConformancePackComplianceDetails",
        "config:getConformancePackComplianceSummary",
        "config:getDiscoveredResourceCounts",
        "config:getOrganizationConfigRuleDetailedStatus",
        "config:getOrganizationConformancePackDetailedStatus",
        "config:getResourceConfigHistory",
```

```
        "config:listAggregateDiscoveredResources",
        "config:listDiscoveredResources",
        "config:listTagsForResource",
        "config:selectAggregateResourceConfig",
        "config:selectResourceConfig",
        "connect:batchGetFlowAssociation",
        "connect:describeContact",
        "connect:describeInstance",
        "connect:describeInstanceAttribute",
        "connect:describePhoneNumber",
        "connect:describeQueue",
        "connect:describeQuickConnect",
        "connect:describeRoutingProfile",
        "connect:describeUser",
        "connect:describeUserHierarchyStructure",
        "connect:getCurrentMetricData",
        "connect:getMetricData",
        "connect:getMetricDataV2",
        "connect:listContactEvaluations",
        "connect:listEvaluationForms",
        "connect:listEvaluationFormVersions",
        "connect:listPhoneNumbersV2",
        "connect:listQueueQuickConnects",
        "connect:listQueues",
        "connect:listQuickConnects",
        "connect:listRoutingProfileQueues",
        "connect:listRoutingProfiles",
        "connect:listSecurityProfiles",
        "connect:listSecurityProfilePermissions",
        "connect:listUsers",
        "connect:listViews",
        "connect:listViewVersions",
        "connect:searchQueues",
        "connect:searchRoutingProfiles",
        "connect:searchUsers",
        "controltower:describeAccountFactoryConfig",
        "controltower:describeCoreService",
        "controltower:describeGuardrail",
        "controltower:describeGuardrailForTarget",
        "controltower:describeManagedAccount",
        "controltower:describeSingleSignOn",
        "controltower:getAvailableUpdates",
        "controltower:getHomeRegion",
        "controltower:getLandingZone",
```

```
        "controltower:getLandingZoneStatus",
        "controltower:listDirectoryGroups",
        "controltower:listEnabledControls",
        "controltower:listGuardrailsForTarget",
        "controltower:listGuardrailViolations",
        "controltower:listLandingZones",
        "controltower:listManagedAccounts",
        "controltower:listManagedAccountsForGuardrail",
        "controltower:listManagedAccountsForParent",
        "controltower:listManagedOrganizationalUnits",
        "controltower:listManagedOrganizationalUnitsForGuardrail",
        "cost-optimization-hub:getPreferences",
        "cost-optimization-hub:getRecommendation",
        "cost-optimization-hub:listEnrollmentStatuses",
        "cost-optimization-hub:listRecommendations",
        "cost-optimization-hub:listRecommendationSummaries",
        "databrew:describeDataset",
        "databrew:describeJob",
        "databrew:describeProject",
        "databrew:describeRecipe",
        "databrew:listDatasets",
        "databrew:listJobRuns",
        "databrew:listJobs",
        "databrew:listProjects",
        "databrew:listRecipes",
        "databrew:listRecipeVersions",
        "databrew:listTagsForResource",
        "datapipeline:describeObjects",
        "datapipeline:describePipelines",
        "datapipeline:getPipelineDefinition",
        "datapipeline:listPipelines",
        "datapipeline:queryObjects",
        "datasync:describeAgent",
        "datasync:describeLocationAzureBlob",
        "datasync:describeLocationEfs",
        "datasync:describeLocationFsxLustre",
        "datasync:describeLocationFsxOntap",
        "datasync:describeLocationFsxOpenZfs",
        "datasync:describeLocationFsxWindows",
        "datasync:describeLocationHdfs",
        "datasync:describeLocationNfs",
        "datasync:describeLocationObjectStorage",
        "datasync:describeLocationS3",
        "datasync:describeLocationSmb",
```

```
        "datasync:describeTask",
        "datasync:describeTaskExecution",
        "datasync:listAgents",
        "datasync:listLocations",
        "datasync:listTaskExecutions",
        "datasync:listTasks",
        "datazone:getAsset",
        "datazone:getAssetType",
        "datazone:getDataSource",
        "datazone:getDataSourceRun",
        "datazone:getDomain",
        "datazone:getEnvironment",
        "datazone:getEnvironmentBlueprint",
        "datazone:getEnvironmentBlueprintConfiguration",
        "datazone:getEnvironmentProfile",
        "datazone:getFormType",
        "datazone:getGlossary",
        "datazone:getGlossaryTerm",
        "datazone:getGroupProfile",
        "datazone:getListing",
        "datazone:getMetadataGenerationRun",
        "datazone:getProject",
        "datazone:getSubscription",
        "datazone:getSubscriptionGrant",
        "datazone:getSubscriptionRequestDetails",
        "datazone:getSubscriptionTarget",
        "datazone:getUserProfile",
        "datazone:listAssetRevisions",
        "datazone:listDataSourceRunActivities",
        "datazone:listDataSourceRuns",
        "datazone:listDataSources",
        "datazone:listDomains",
        "datazone:listEnvironmentBlueprintConfigurations",
        "datazone:listEnvironmentBlueprints",
        "datazone:listEnvironmentProfiles",
        "datazone:listEnvironments",
        "datazone:listMetadataGenerationRuns",
        "datazone:listProjectMemberships",
        "datazone:listProjects",
        "datazone:listSubscriptionGrants",
        "datazone:listSubscriptionRequests",
        "datazone:listSubscriptions",
        "datazone:listSubscriptionTargets",
        "datazone:searchGroupProfiles",
```

```
        "datazone:searchUserProfiles",
        "dax:describeClusters",
        "dax:describeDefaultParameters",
        "dax:describeEvents",
        "dax:describeParameterGroups",
        "dax:describeParameters",
        "dax:describeSubnetGroups",
        "deadline:listAvailableMeteredProducts",
        "deadline:listBudgets",
        "deadline:listFarmMembers",
        "deadline:listFarms",
        "deadline:listFleetMembers",
        "deadline:listFleets",
        "deadline:listJobMembers",
        "deadline:listJobs",
        "deadline:listLicenseEndpoints",
        "deadline:listMeteredProducts",
        "deadline:listMonitors",
        "deadline:listQueueEnvironments",
        "deadline:listQueueFleetAssociations",
        "deadline:listQueueMembers",
        "deadline:listQueues",
        "deadline:listStorageProfiles",
        "deadline:listWorkers",
        "detective:getMembers",
        "detective:listGraphs",
        "detective:listInvitations",
        "detective:listMembers",
        "devicefarm:getAccountSettings",
        "devicefarm:getDevice",
        "devicefarm:getDevicePool",
        "devicefarm:getDevicePoolCompatibility",
        "devicefarm:getJob",
        "devicefarm:getProject",
        "devicefarm:getRemoteAccessSession",
        "devicefarm:getRun",
        "devicefarm:getSuite",
        "devicefarm:getTest",
        "devicefarm:getTestGridProject",
        "devicefarm:getTestGridSession",
        "devicefarm:getUpload",
        "devicefarm:listArtifacts",
        "devicefarm:listDevicePools",
        "devicefarm:listDevices",
```

```
        "devicefarm:listJobs",
        "devicefarm:listProjects",
        "devicefarm:listRemoteAccessSessions",
        "devicefarm:listRuns",
        "devicefarm:listSamples",
        "devicefarm:listSuites",
        "devicefarm:listTestGridProjects",
        "devicefarm:listTestGridSessionActions",
        "devicefarm:listTestGridSessionArtifacts",
        "devicefarm:listTestGridSessions",
        "devicefarm:listTests",
        "devicefarm:listUniqueProblems",
        "devicefarm:listUploads",
        "directconnect:describeConnectionLoa",
        "directconnect:describeConnections",
        "directconnect:describeConnectionsOnInterconnect",
        "directconnect:describeCustomerMetadata",
        "directconnect:describeDirectConnectGatewayAssociationProposals",
        "directconnect:describeDirectConnectGatewayAssociations",
        "directconnect:describeDirectConnectGatewayAttachments",
        "directconnect:describeDirectConnectGateways",
        "directconnect:describeHostedConnections",
        "directconnect:describeInterconnectLoa",
        "directconnect:describeInterconnects",
        "directconnect:describeLags",
        "directconnect:describeLoa",
        "directconnect:describeLocations",
        "directconnect:describeRouterConfiguration",
        "directconnect:describeVirtualGateways",
        "directconnect:describeVirtualInterfaces",
        "directconnect:listVirtualInterfaceTestHistory",
        "dlm:getLifecyclePolicies",
        "dlm:getLifecyclePolicy",
        "dms:describeAccountAttributes",
        "dms:describeApplicableIndividualAssessments",
        "dms:describeConnections",
        "dms:describeEndpoints",
        "dms:describeEndpointSettings",
        "dms:describeEndpointTypes",
        "dms:describeEventCategories",
        "dms:describeEvents",
        "dms:describeEventSubscriptions",
        "dms:describeFleetAdvisorCollectors",
        "dms:describeFleetAdvisorDatabases",
```

```
        "dms:describeFleetAdvisorLsaAnalysis",
        "dms:describeFleetAdvisorSchemaObjectSummary",
        "dms:describeFleetAdvisorSchemas",
        "dms:describeOrderableReplicationInstances",
        "dms:describePendingMaintenanceActions",
        "dms:describeRefreshSchemasStatus",
        "dms:describeReplicationInstances",
        "dms:describeReplicationInstanceTaskLogs",
        "dms:describeReplicationSubnetGroups",
        "dms:describeReplicationTaskAssessmentResults",
        "dms:describeReplicationTaskAssessmentRuns",
        "dms:describeReplicationTaskIndividualAssessments",
        "dms:describeReplicationTasks",
        "dms:describeSchemas",
        "dms:describeTableStatistics",
        "docdb-elastic:getCluster",
        "docdb-elastic:getClusterSnapshot",
        "docdb-elastic:listClusters",
        "docdb-elastic:listClusterSnapshots",
        "drs:describeJobLogItems",
        "drs:describeJobs",
        "drs:describeLaunchConfigurationTemplates",
        "drs:describeRecoveryInstances",
        "drs:describeRecoverySnapshots",
        "drs:describeReplicationConfigurationTemplates",
        "drs:describeSourceNetworks",
        "drs:describeSourceServers",
        "drs:getLaunchConfiguration",
        "drs:getReplicationConfiguration",
        "drs:listExtensibleSourceServers",
        "drs:listLaunchActions",
        "drs:listStagingAccounts",
        "ds:describeClientAuthenticationSettings",
        "ds:describeConditionalForwarders",
        "ds:describeDirectories",
        "ds:describeDomainControllers",
        "ds:describeEventTopics",
        "ds:describeHybridADUpdate",
        "ds:describeLDAPSSettings",
        "ds:describeSharedDirectories",
        "ds:describeSnapshots",
        "ds:describeTrusts",
        "ds:getDirectoryLimits",
        "ds:getSnapshotLimits",
```

```
        "ds:listIpRoutes",
        "ds:listSchemaExtensions",
        "ds:listTagsForResource",
        "dynamodb:describeBackup",
        "dynamodb:describeContinuousBackups",
        "dynamodb:describeContributorInsights",
        "dynamodb:describeExport",
        "dynamodb:describeGlobalTable",
        "dynamodb:describeGlobalTableSettings",
        "dynamodb:describeImport",
        "dynamodb:describeKinesisStreamingDestination",
        "dynamodb:describeLimits",
        "dynamodb:describeStream",
        "dynamodb:describeTable",
        "dynamodb:describeTableReplicaAutoScaling",
        "dynamodb:describeTimeToLive",
        "dynamodb:getResourcePolicy",
        "dynamodb:listBackups",
        "dynamodb:listContributorInsights",
        "dynamodb:listExports",
        "dynamodb:listGlobalTables",
        "dynamodb:listImports",
        "dynamodb:listStreams",
        "dynamodb:listTables",
        "dynamodb:listTagsOfResource",
        "ec2:describeAccountAttributes",
        "ec2:describeAddresses",
        "ec2:describeAddressesAttribute",
        "ec2:describeAddressTransfers",
        "ec2:describeAggregateIdFormat",
        "ec2:describeAvailabilityZones",
        "ec2:describeBundleTasks",
        "ec2:describeByoipCidrs",
        "ec2:describeCapacityBlockOfferings",
        "ec2:describeCapacityReservationFleets",
        "ec2:describeCapacityReservations",
        "ec2:describeCarrierGateways",
        "ec2:describeClassicLinkInstances",
        "ec2:describeClientVpnAuthorizationRules",
        "ec2:describeClientVpnConnections",
        "ec2:describeClientVpnEndpoints",
        "ec2:describeClientVpnRoutes",
        "ec2:describeClientVpnTargetNetworks",
        "ec2:describeCoipPools",
```

```
        "ec2:describeConversionTasks",
        "ec2:describeCustomerGateways",
        "ec2:describeDhcpOptions",
        "ec2:describeEgressOnlyInternetGateways",
        "ec2:describeExportImageTasks",
        "ec2:describeExportTasks",
        "ec2:describeFastLaunchImages",
        "ec2:describeFastSnapshotRestores",
        "ec2:describeFleetHistory",
        "ec2:describeFleetInstances",
        "ec2:describeFleets",
        "ec2:describeFlowLogs",
        "ec2:describeFpgaImageAttribute",
        "ec2:describeFpgaImages",
        "ec2:describeHostReservationOfferings",
        "ec2:describeHostReservations",
        "ec2:describeHosts",
        "ec2:describeIamInstanceProfileAssociations",
        "ec2:describeIdentityIdFormat",
        "ec2:describeIdFormat",
        "ec2:describeImageAttribute",
        "ec2:describeImages",
        "ec2:describeImportImageTasks",
        "ec2:describeImportSnapshotTasks",
        "ec2:describeInstanceAttribute",
        "ec2:describeInstanceConnectEndpoints",
        "ec2:describeInstanceCreditSpecifications",
        "ec2:describeInstanceEventNotificationAttributes",
        "ec2:describeInstanceEventWindows",
        "ec2:describeInstances",
        "ec2:describeInstanceStatus",
        "ec2:describeInstanceTypeOfferings",
        "ec2:describeInstanceTypes",
        "ec2:describeInternetGateways",
        "ec2:describeIpamByoasn",
        "ec2:describeIpamExternalResourceVerificationTokens",
        "ec2:describeIpamPools",
        "ec2:describeIpamResourceDiscoveries",
        "ec2:describeIpamResourceDiscoveryAssociations",
        "ec2:describeIpams",
        "ec2:describeIpamScopes",
        "ec2:describeIpv6Pools",
        "ec2:describeKeyPairs",
        "ec2:describeLaunchTemplates",
```

```
        "ec2:describeLaunchTemplateVersions",
        "ec2:describeLocalGatewayRouteTables",
        "ec2:describeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:describeLocalGatewayRouteTableVpcAssociations",
        "ec2:describeLocalGateways",
        "ec2:describeLocalGatewayVirtualInterfaceGroups",
        "ec2:describeLocalGatewayVirtualInterfaces",
        "ec2:describeManagedPrefixLists",
        "ec2:describeMovingAddresses",
        "ec2:describeNatGateways",
        "ec2:describeNetworkAcls",
        "ec2:describeNetworkInsightsAccessScopeAnalyses",
        "ec2:describeNetworkInsightsAccessScopes",
        "ec2:describeNetworkInsightsAnalyses",
        "ec2:describeNetworkInsightsPaths",
        "ec2:describeNetworkInterfaceAttribute",
        "ec2:describeNetworkInterfaces",
        "ec2:describePlacementGroups",
        "ec2:describePrefixLists",
        "ec2:describePrincipalIdFormat",
        "ec2:describePublicIpv4Pools",
        "ec2:describeRegions",
        "ec2:describeReplaceRootVolumeTasks",
        "ec2:describeReservedInstances",
        "ec2:describeReservedInstancesListings",
        "ec2:describeReservedInstancesModifications",
        "ec2:describeReservedInstancesOfferings",
        "ec2:describeRouteServerEndpoints",
        "ec2:describeRouteServerPeers",
        "ec2:describeRouteServers",
        "ec2:describeRouteTables",
        "ec2:describeScheduledInstanceAvailability",
        "ec2:describeScheduledInstances",
        "ec2:describeSecurityGroupReferences",
        "ec2:describeSecurityGroupRules",
        "ec2:describeSecurityGroups",
        "ec2:describeServiceLinkVirtualInterfaces",
        "ec2:describeSnapshotAttribute",
        "ec2:describeSnapshots",
        "ec2:describeSnapshotTierStatus",
        "ec2:describeSpotDatafeedSubscription",
        "ec2:describeSpotFleetInstances",
        "ec2:describeSpotFleetRequestHistory",
        "ec2:describeSpotFleetRequests",
```

```
        "ec2:describeSpotInstanceRequests",
        "ec2:describeSpotPriceHistory",
        "ec2:describeStaleSecurityGroups",
        "ec2:describeStoreImageTasks",
        "ec2:describeSubnets",
        "ec2:describeTags",
        "ec2:describeTrafficMirrorFilterRules",
        "ec2:describeTrafficMirrorFilters",
        "ec2:describeTrafficMirrorSessions",
        "ec2:describeTrafficMirrorTargets",
        "ec2:describeTransitGatewayAttachments",
        "ec2:describeTransitGatewayConnectPeers",
        "ec2:describeTransitGatewayMulticastDomains",
        "ec2:describeTransitGatewayPeeringAttachments",
        "ec2:describeTransitGatewayPolicyTables",
        "ec2:describeTransitGatewayRouteTableAnnouncements",
        "ec2:describeTransitGatewayRouteTables",
        "ec2:describeTransitGateways",
        "ec2:describeTransitGatewayVpcAttachments",
        "ec2:describeVerifiedAccessEndpoints",
        "ec2:describeVerifiedAccessGroups",
        "ec2:describeVerifiedAccessInstanceLoggingConfigurations",
        "ec2:describeVerifiedAccessInstances",
        "ec2:describeVerifiedAccessTrustProviders",
        "ec2:describeVolumeAttribute",
        "ec2:describeVolumes",
        "ec2:describeVolumesModifications",
        "ec2:describeVolumeStatus",
        "ec2:describeVpcAttribute",
        "ec2:describeVpcBlockPublicAccessExclusions",
        "ec2:describeVpcBlockPublicAccessOptions",
        "ec2:describeVpcClassicLink",
        "ec2:describeVpcClassicLinkDnsSupport",
        "ec2:describeVpcEndpointAssociations",
        "ec2:describeVpcEndpointConnectionNotifications",
        "ec2:describeVpcEndpointConnections",
        "ec2:describeVpcEndpoints",
        "ec2:describeVpcEndpointServiceConfigurations",
        "ec2:describeVpcEndpointServicePermissions",
        "ec2:describeVpcEndpointServices",
        "ec2:describeVpcPeeringConnections",
        "ec2:describeVpcs",
        "ec2:describeVpnConnections",
        "ec2:describeVpnGateways",
```

```
        "ec2:getAssociatedEnclaveCertificateIamRoles",
        "ec2:getAssociatedIpv6PoolCidrs",
        "ec2:getCapacityReservationUsage",
        "ec2:getCoipPoolUsage",
        "ec2:getConsoleOutput",
        "ec2:getConsoleScreenshot",
        "ec2:getDefaultCreditSpecification",
        "ec2:getEbsDefaultKmsKeyId",
        "ec2:getEbsEncryptionByDefault",
        "ec2:getGroupsForCapacityReservation",
        "ec2:getHostReservationPurchasePreview",
        "ec2:getImageBlockPublicAccessState",
        "ec2:getInstanceTypesFromInstanceRequirements",
        "ec2:getIpamAddressHistory",
        "ec2:getIpamDiscoveredAccounts",
        "ec2:getIpamDiscoveredPublicAddresses",
        "ec2:getIpamDiscoveredResourceCidrs",
        "ec2:getIpamPoolAllocations",
        "ec2:getIpamPoolCidrs",
        "ec2:getIpamResourceCidrs",
        "ec2:getLaunchTemplateData",
        "ec2:getManagedPrefixListAssociations",
        "ec2:getManagedPrefixListEntries",
        "ec2:getNetworkInsightsAccessScopeContent",
        "ec2:getReservedInstancesExchangeQuote",
        "ec2:getRouteServerAssociations",
        "ec2:getRouteServerPropagations",
        "ec2:getRouteServerRoutingDatabase",
        "ec2:getSerialConsoleAccessStatus",
        "ec2:getSpotPlacementScores",
        "ec2:getSubnetCidrReservations",
        "ec2:getTransitGatewayMulticastDomainAssociations",
        "ec2:getTransitGatewayPrefixListReferences",
        "ec2:getVerifiedAccessEndpointPolicy",
        "ec2:getVerifiedAccessGroupPolicy",
        "ec2:listImagesInRecycleBin",
        "ec2:listSnapshotsInRecycleBin",
        "ec2:searchLocalGatewayRoutes",
        "ec2:searchTransitGatewayMulticastGroups",
        "ec2:searchTransitGatewayRoutes",
        "ecr-public:describeImages",
        "ecr-public:describeImageTags",
        "ecr-public:describeRegistries",
        "ecr-public:describeRepositories",
```

```
        "ecr-public:getRegistryCatalogData",
        "ecr-public:getRepositoryCatalogData",
        "ecr-public:getRepositoryPolicy",
        "ecr-public:listTagsForResource",
        "ecr:batchCheckLayerAvailability",
        "ecr:batchGetRepositoryScanningConfiguration",
        "ecr:describeImageReplicationStatus",
        "ecr:describeImages",
        "ecr:describeImageScanFindings",
        "ecr:describePullThroughCacheRules",
        "ecr:describeRegistry",
        "ecr:describeRepositories",
        "ecr:getLifecyclePolicy",
        "ecr:getLifecyclePolicyPreview",
        "ecr:getRegistryPolicy",
        "ecr:getRegistryScanningConfiguration",
        "ecr:getRepositoryPolicy",
        "ecr:listImages",
        "ecr:listTagsForResource",
        "ecs:describeCapacityProviders",
        "ecs:describeClusters",
        "ecs:describeContainerInstances",
        "ecs:describeServiceDeployments",
        "ecs:describeServiceRevisions",
        "ecs:describeServices",
        "ecs:describeTaskDefinition",
        "ecs:describeTasks",
        "ecs:describeTaskSets",
        "ecs:getTaskProtection",
        "ecs:listAccountSettings",
        "ecs:listAttributes",
        "ecs:listClusters",
        "ecs:listContainerInstances",
        "ecs:listServiceDeployments",
        "ecs:listServices",
        "ecs:listServicesByNamespace",
        "ecs:listTagsForResource",
        "ecs:listTaskDefinitionFamilies",
        "ecs:listTaskDefinitions",
        "ecs:listTasks"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup2",
      "Action" : [
        "eks:describeAccessEntry",
        "eks:describeAddon",
        "eks:describeAddonConfiguration",
        "eks:describeAddonVersions",
        "eks:describeCluster",
        "eks:describeEksAnywhereSubscription",
        "eks:describeFargateProfile",
        "eks:describeIdentityProviderConfig",
        "eks:describeInsight",
        "eks:describeNodegroup",
        "eks:describePodIdentityAssociation",
        "eks:describeUpdate",
        "eks:listAccessEntries",
        "eks:listAccessPolicies",
        "eks:listAddons",
        "eks:listAssociatedAccessPolicies",
        "eks:listClusters",
        "eks:listEksAnywhereSubscriptions",
        "eks:listFargateProfiles",
        "eks:listIdentityProviderConfigs",
        "eks:listInsights",
        "eks:listNodegroups",
        "eks:listPodIdentityAssociations",
        "eks:listUpdates",
        "elasticache:describeCacheClusters",
        "elasticache:describeCacheEngineVersions",
        "elasticache:describeCacheParameterGroups",
        "elasticache:describeCacheParameters",
        "elasticache:describeCacheSecurityGroups",
        "elasticache:describeCacheSubnetGroups",
        "elasticache:describeEngineDefaultParameters",
        "elasticache:describeEvents",
        "elasticache:describeGlobalReplicationGroups",
        "elasticache:describeReplicationGroups",
        "elasticache:describeReservedCacheNodes",
        "elasticache:describeReservedCacheNodesOfferings",
        "elasticache:describeServerlessCaches",
        "elasticache:describeServerlessCacheSnapshots",
        "elasticache:describeServiceUpdates",
```

```
        "elasticache:describeSnapshots",
        "elasticache:describeUpdateActions",
        "elasticache:describeUserGroups",
        "elasticache:describeUsers",
        "elasticache:listAllowedNodeTypeModifications",
        "elasticache:listTagsForResource",
        "elasticbeanstalk:checkDNSAvailability",
        "elasticbeanstalk:describeAccountAttributes",
        "elasticbeanstalk:describeApplications",
        "elasticbeanstalk:describeApplicationVersions",
        "elasticbeanstalk:describeConfigurationOptions",
        "elasticbeanstalk:describeEnvironmentHealth",
        "elasticbeanstalk:describeEnvironmentManagedActionHistory",
        "elasticbeanstalk:describeEnvironmentManagedActions",
        "elasticbeanstalk:describeEnvironmentResources",
        "elasticbeanstalk:describeEnvironments",
        "elasticbeanstalk:describeEvents",
        "elasticbeanstalk:describeInstancesHealth",
        "elasticbeanstalk:describePlatformVersion",
        "elasticbeanstalk:listAvailableSolutionStacks",
        "elasticbeanstalk:listPlatformBranches",
        "elasticbeanstalk:listPlatformVersions",
        "elasticbeanstalk:validateConfigurationSettings",
        "elasticfilesystem:describeAccessPoints",
        "elasticfilesystem:describeBackupPolicy",
        "elasticfilesystem:describeFileSystemPolicy",
        "elasticfilesystem:describeFileSystems",
        "elasticfilesystem:describeLifecycleConfiguration",
        "elasticfilesystem:describeMountTargets",
        "elasticfilesystem:describeMountTargetSecurityGroups",
        "elasticfilesystem:describeReplicationConfigurations",
        "elasticfilesystem:describeTags",
        "elasticfilesystem:listTagsForResource",
        "elasticloadbalancing:describeAccountLimits",
        "elasticloadbalancing:describeInstanceHealth",
        "elasticloadbalancing:describeListenerCertificates",
        "elasticloadbalancing:describeListeners",
        "elasticloadbalancing:describeLoadBalancerAttributes",
        "elasticloadbalancing:describeLoadBalancerPolicies",
        "elasticloadbalancing:describeLoadBalancerPolicyTypes",
        "elasticloadbalancing:describeLoadBalancers",
        "elasticloadbalancing:describeRules",
        "elasticloadbalancing:describeSSLPolicies",
        "elasticloadbalancing:describeTags",
```

```
        "elasticloadbalancing:describeTargetGroupAttributes",
        "elasticloadbalancing:describeTargetGroups",
        "elasticloadbalancing:describeTargetHealth",
        "elasticloadbalancing:describeTrustStoreAssociations",
        "elasticloadbalancing:describeTrustStoreRevocations",
        "elasticloadbalancing:describeTrustStores",
        "elasticmapreduce:describeCluster",
        "elasticmapreduce:describeNotebookExecution",
        "elasticmapreduce:describePersistentAppUI",
        "elasticmapreduce:describeReleaseLabel",
        "elasticmapreduce:describeSecurityConfiguration",
        "elasticmapreduce:describeStep",
        "elasticmapreduce:describeStudio",
        "elasticmapreduce:getAutoTerminationPolicy",
        "elasticmapreduce:getBlockPublicAccessConfiguration",
        "elasticmapreduce:getManagedScalingPolicy",
        "elasticmapreduce:getStudioSessionMapping",
        "elasticmapreduce:listBootstrapActions",
        "elasticmapreduce:listClusters",
        "elasticmapreduce:listInstanceFleets",
        "elasticmapreduce:listInstanceGroups",
        "elasticmapreduce:listInstances",
        "elasticmapreduce:listNotebookExecutions",
        "elasticmapreduce:listReleaseLabels",
        "elasticmapreduce:listSecurityConfigurations",
        "elasticmapreduce:listSteps",
        "elasticmapreduce:listStudios",
        "elasticmapreduce:listStudioSessionMappings",
        "elasticmapreduce:listSupportedInstanceTypes",
        "elastictranscoder:listJobsByPipeline",
        "elastictranscoder:listJobsByStatus",
        "elastictranscoder:listPipelines",
        "elastictranscoder:listPresets",
        "elastictranscoder:readPipeline",
        "elastictranscoder:readPreset",
        "emr-containers:describeJobRun",
        "emr-containers:describeJobTemplate",
        "emr-containers:describeManagedEndpoint",
        "emr-containers:describeVirtualCluster",
        "emr-containers:listJobRuns",
        "emr-containers:listJobTemplates",
        "emr-containers:listManagedEndpoints",
        "emr-containers:listVirtualClusters",
        "emr-serverless:getApplication",
```

```
        "emr-serverless:getJobRun",
        "emr-serverless:listApplications",
        "es:describeDomain",
        "es:describeDomainAutoTunes",
        "es:describeDomainChangeProgress",
        "es:describeDomainConfig",
        "es:describeDomainHealth",
        "es:describeDomainNodes",
        "es:describeDomains",
        "es:describeDryRunProgress",
        "es:describeElasticsearchDomain",
        "es:describeElasticsearchDomainConfig",
        "es:describeElasticsearchDomains",
        "es:getDomainMaintenanceStatus",
        "es:describeInboundConnections",
        "es:describeInstanceTypeLimits",
        "es:describeOutboundConnections",
        "es:describePackages",
        "es:describeReservedInstanceOfferings",
        "es:describeReservedInstances",
        "es:describeVpcEndpoints",
        "es:getCompatibleVersions",
        "es:getPackageVersionHistory",
        "es:getUpgradeHistory",
        "es:getUpgradeStatus",
        "es:listDomainMaintenances",
        "es:listDomainNames",
        "es:listDomainsForPackage",
        "es:listInstanceTypeDetails",
        "es:listPackagesForDomain",
        "es:listScheduledActions",
        "es:listTags",
        "es:listVersions",
        "es:listVpcEndpointAccess",
        "es:listVpcEndpoints",
        "es:listVpcEndpointsForDomain",
        "events:describeApiDestination",
        "events:describeArchive",
        "events:describeConnection",
        "events:describeEndpoint",
        "events:describeEventBus",
        "events:describeEventSource",
        "events:describePartnerEventSource",
        "events:describeReplay",
```

```
        "events:describeRule",
        "events:listApiDestinations",
        "events:listArchives",
        "events:listConnections",
        "events:listEndpoints",
        "events:listEventBuses",
        "events:listEventSources",
        "events:listPartnerEventSourceAccounts",
        "events:listPartnerEventSources",
        "events:listReplays",
        "events:listRuleNamesByTarget",
        "events:listRules",
        "events:listTargetsByRule",
        "events:testEventPattern",
        "evidently:getExperiment",
        "evidently:getFeature",
        "evidently:getLaunch",
        "evidently:getProject",
        "evidently:getSegment",
        "evidently:listExperiments",
        "evidently:listFeatures",
        "evidently:listLaunches",
        "evidently:listProjects",
        "evidently:listSegmentReferences",
        "evidently:listSegments",
        "firehose:describeDeliveryStream",
        "firehose:listDeliveryStreams",
        "fis:getAction",
        "fis:getExperiment",
        "fis:getExperimentTargetAccountConfiguration",
        "fis:getExperimentTemplate",
        "fis:getSafetyLever",
        "fis:getTargetAccountConfiguration",
        "fis:listActions",
        "fis:listExperimentResolvedTargets",
        "fis:listExperimentTargetAccountConfigurations",
        "fis:listExperiments",
        "fis:listExperimentTemplates",
        "fis:listTargetAccountConfigurations",
        "fms:getAdminAccount",
        "fms:getAdminScope",
        "fms:getAppsList",
        "fms:getComplianceDetail",
        "fms:getNotificationChannel",
```

```
        "fms:getProtocolsList",
        "fms:getPolicy",
        "fms:getProtectionStatus",
        "fms:getResourceSet",
        "fms:getThirdPartyFirewallAssociationStatus",
        "fms:getViolationDetails",
        "fms:listAdminAccountsForOrganization",
        "fms:listAdminsManagingAccount",
        "fms:listAppsLists",
        "fms:listComplianceStatus",
        "fms:listDiscoveredResources",
        "fms:listMemberAccounts",
        "fms:listProtocolsLists",
        "fms:listPolicies",
        "fms:listResourceSetResources",
        "fms:listResourceSets",
        "fms:listThirdPartyFirewallFirewallPolicies",
        "forecast:describeDataset",
        "forecast:describeDatasetGroup",
        "forecast:describeDatasetImportJob",
        "forecast:describeForecast",
        "forecast:describeForecastExportJob",
        "forecast:describePredictor",
        "forecast:getAccuracyMetrics",
        "forecast:listDatasetGroups",
        "forecast:listDatasetImportJobs",
        "forecast:listDatasets",
        "forecast:listForecastExportJobs",
        "forecast:listForecasts",
        "forecast:listPredictors",
        "freetier:getFreeTierUsage",
        "fsx:describeBackups",
        "fsx:describeDataRepositoryAssociations",
        "fsx:describeDataRepositoryTasks",
        "fsx:describeFileCaches",
        "fsx:describeFileSystems",
        "fsx:describeS3AccessPointAttachments",
        "fsx:describeSnapshots",
        "fsx:describeStorageVirtualMachines",
        "fsx:describeVolumes",
        "fsx:listTagsForResource",
        "gamelift:describeAlias",
        "gamelift:describeBuild",
        "gamelift:describeEC2InstanceLimits",
```

```
        "gamelift:describeFleetAttributes",
        "gamelift:describeFleetCapacity",
        "gamelift:describeFleetEvents",
        "gamelift:describeFleetLocationAttributes",
        "gamelift:describeFleetLocationCapacity",
        "gamelift:describeFleetLocationUtilization",
        "gamelift:describeFleetPortSettings",
        "gamelift:describeFleetUtilization",
        "gamelift:describeGameServer",
        "gamelift:describeGameServerGroup",
        "gamelift:describeGameSessionDetails",
        "gamelift:describeGameSessionPlacement",
        "gamelift:describeGameSessionQueues",
        "gamelift:describeGameSessions",
        "gamelift:describeInstances",
        "gamelift:describeMatchmaking",
        "gamelift:describeMatchmakingConfigurations",
        "gamelift:describeMatchmakingRuleSets",
        "gamelift:describePlayerSessions",
        "gamelift:describeRuntimeConfiguration",
        "gamelift:describeScalingPolicies",
        "gamelift:describeScript",
        "gamelift:listAliases",
        "gamelift:listBuilds",
        "gamelift:listFleets",
        "gamelift:listGameServerGroups",
        "gamelift:listGameServers",
        "gamelift:listScripts",
        "gamelift:resolveAlias",
        "geo:calculateRoute",
        "geo:calculateRouteMatrix",
        "geo:describeMap",
        "geo:describePlaceIndex",
        "geo:describeRouteCalculator",
        "geo:describeTracker",
        "geo:getMapGlyphs",
        "geo:getMapSprites",
        "geo:getMapStyleDescriptor",
        "geo:getMapTile",
        "geo:getPlace",
        "geo:listGeofenceCollections",
        "geo:listMaps",
        "geo:listPlaceIndexes",
        "geo:listRouteCalculators",
```

```
        "geo:listTrackerConsumers",
        "geo:searchPlaceIndexForPosition",
        "geo:searchPlaceIndexForSuggestions",
        "geo:searchPlaceIndexForText",
        "geo-maps:getStaticMap",
        "geo-maps:getTile",
        "geo-places:autocomplete",
        "geo-places:geocode",
        "geo-places:getPlace",
        "geo-places:reverseGeocode",
        "geo-places:searchNearby",
        "geo-places:searchText",
        "geo-places:suggest",
        "geo-routes:calculateIsolines",
        "geo-routes:calculateRouteMatrix",
        "geo-routes:calculateRoutes",
        "geo-routes:optimizeWaypoints",
        "geo-routes:snapToRoads",
        "glacier:describeJob",
        "glacier:describeVault",
        "glacier:getDataRetrievalPolicy",
        "glacier:getVaultAccessPolicy",
        "glacier:getVaultLock",
        "glacier:getVaultNotifications",
        "glacier:listJobs",
        "glacier:listTagsForVault",
        "glacier:listVaults",
        "globalaccelerator:describeAccelerator",
        "globalaccelerator:describeAcceleratorAttributes",
        "globalaccelerator:describeCrossAccountAttachment",
        "globalaccelerator:describeCustomRoutingAccelerator",
        "globalaccelerator:describeCustomRoutingAcceleratorAttributes",
        "globalaccelerator:describeCustomRoutingEndpointGroup",
        "globalaccelerator:describeCustomRoutingListener",
        "globalaccelerator:describeEndpointGroup",
        "globalaccelerator:describeListener",
        "globalaccelerator:listAccelerators",
        "globalaccelerator:listByoipCidrs",
        "globalaccelerator:listCrossAccountAttachments",
        "globalaccelerator:listCrossAccountResourceAccounts",
        "globalaccelerator:listCrossAccountResources",
        "globalaccelerator:listCustomRoutingAccelerators",
        "globalaccelerator:listCustomRoutingEndpointGroups",
        "globalaccelerator:listCustomRoutingListeners",
```

```
        "globalaccelerator:listCustomRoutingPortMappings",
        "globalaccelerator:listCustomRoutingPortMappingsByDestination",
        "globalaccelerator:listEndpointGroups",
        "globalaccelerator:listListeners",
        "glue:batchGetBlueprints",
        "glue:batchGetCrawlers",
        "glue:batchGetDevEndpoints",
        "glue:batchGetJobs",
        "glue:batchGetPartition",
        "glue:batchGetTriggers",
        "glue:batchGetWorkflows",
        "glue:checkSchemaVersionValidity",
        "glue:batchGetTableOptimizer",
        "glue:getBlueprint",
        "glue:getBlueprintRun",
        "glue:getBlueprintRuns",
        "glue:getCatalogImportStatus",
        "glue:getClassifier",
        "glue:getClassifiers",
        "glue:getColumnStatisticsForPartition",
        "glue:getColumnStatisticsForTable",
        "glue:getColumnStatisticsTaskRun",
        "glue:getColumnStatisticsTaskRuns",
        "glue:getCrawler",
        "glue:getCrawlerMetrics",
        "glue:getCrawlers",
        "glue:getCustomEntityType",
        "glue:getDatabase",
        "glue:getDatabases",
        "glue:getDataCatalogEncryptionSettings",
        "glue:getDataflowGraph",
        "glue:getDataQualityResult",
        "glue:getDataQualityRuleRecommendationRun",
        "glue:getDataQualityRuleset",
        "glue:getDataQualityRulesetEvaluationRun",
        "glue:getDevEndpoint",
        "glue:getDevEndpoints",
        "glue:getJob",
        "glue:getJobBookmark",
        "glue:getJobRun",
        "glue:getJobRuns",
        "glue:getJobs",
        "glue:getMapping",
        "glue:getMLTaskRun",
```

```
        "glue:getMLTaskRuns",
        "glue:getMLTransform",
        "glue:getMLTransforms",
        "glue:getPartition",
        "glue:getPartitionIndexes",
        "glue:getPartitions",
        "glue:getRegistry",
        "glue:getResourcePolicies",
        "glue:getResourcePolicy",
        "glue:getSchema",
        "glue:getSchemaByDefinition",
        "glue:getSchemaVersion",
        "glue:getSchemaVersionsDiff",
        "glue:getSecurityConfiguration",
        "glue:getSecurityConfigurations",
        "glue:getSession",
        "glue:getStatement",
        "glue:getTable",
        "glue:getTableOptimizer",
        "glue:getTables",
        "glue:getTableVersions",
        "glue:getTrigger",
        "glue:getTriggers",
        "glue:getUserDefinedFunction",
        "glue:getUserDefinedFunctions",
        "glue:getWorkflow",
        "glue:getWorkflowRun",
        "glue:getWorkflowRuns",
        "glue:listColumnStatisticsTaskRuns",
        "glue:listCrawlers",
        "glue:listCrawls",
        "glue:listDataQualityResults",
        "glue:listDataQualityRuleRecommendationRuns",
        "glue:listDataQualityRulesetEvaluationRuns",
        "glue:listDataQualityRulesets",
        "glue:listDevEndpoints",
        "glue:listMLTransforms",
        "glue:listRegistries",
        "glue:listSchemas",
        "glue:listSchemaVersions",
        "glue:listSessions",
        "glue:listStatements",
        "glue:listTableOptimizerRuns",
        "glue:listTriggers",
```

```
        "glue:querySchemaVersionMetadata",
        "glue:getTableVersion",
        "grafana:describeWorkspace",
        "grafana:describeWorkspaceAuthentication",
        "grafana:listPermissions",
        "grafana:listVersions",
        "grafana:listWorkspaces",
        "greengrass:getConnectivityInfo",
        "greengrass:getCoreDefinition",
        "greengrass:getCoreDefinitionVersion",
        "greengrass:getDeploymentStatus",
        "greengrass:getDeviceDefinition",
        "greengrass:getDeviceDefinitionVersion",
        "greengrass:getFunctionDefinition",
        "greengrass:getFunctionDefinitionVersion",
        "greengrass:getGroup",
        "greengrass:getGroupCertificateAuthority",
        "greengrass:getGroupVersion",
        "greengrass:getLoggerDefinition",
        "greengrass:getLoggerDefinitionVersion",
        "greengrass:getResourceDefinitionVersion",
        "greengrass:getServiceRoleForAccount",
        "greengrass:getSubscriptionDefinition",
        "greengrass:getSubscriptionDefinitionVersion",
        "greengrass:listCoreDefinitions",
        "greengrass:listCoreDefinitionVersions",
        "greengrass:listDeployments",
        "greengrass:listDeviceDefinitions",
        "greengrass:listDeviceDefinitionVersions",
        "greengrass:listFunctionDefinitions",
        "greengrass:listFunctionDefinitionVersions",
        "greengrass:listGroups",
        "greengrass:listGroupVersions",
        "greengrass:listLoggerDefinitions",
        "greengrass:listLoggerDefinitionVersions",
        "greengrass:listResourceDefinitions",
        "greengrass:listResourceDefinitionVersions",
        "greengrass:listSubscriptionDefinitions",
        "greengrass:listSubscriptionDefinitionVersions",
        "guardduty:describeMalwareScans",
        "guardduty:describePublishingDestination",
        "guardduty:getCoverageStatistics",
        "guardduty:getDetector",
        "guardduty:getFilter",
```

```
        "guardduty:getFindings",
        "guardduty:getFindingsStatistics",
        "guardduty:getInvitationsCount",
        "guardduty:getIPSet",
        "guardduty:getMalwareScanSettings",
        "guardduty:getMasterAccount",
        "guardduty:getMemberDetectors",
        "guardduty:getMembers",
        "guardduty:getOrganizationStatistics",
        "guardduty:getRemainingFreeTrialDays",
        "guardduty:getThreatIntelSet",
        "guardduty:listCoverage",
        "guardduty:listDetectors",
        "guardduty:listFilters",
        "guardduty:listFindings",
        "guardduty:listInvitations",
        "guardduty:listIPSets",
        "guardduty:listMembers",
        "guardduty:listThreatIntelSets",
        "health:describeAffectedAccountsForOrganization",
        "health:describeAffectedEntities",
        "health:describeAffectedEntitiesForOrganization",
        "health:describeEntityAggregates",
        "health:describeEntityAggregatesForOrganization",
        "health:describeEventAggregates",
        "health:describeEventDetails",
        "health:describeEventDetailsForOrganization",
        "health:describeEvents",
        "health:describeEventsForOrganization",
        "health:describeEventTypes",
        "health:describeHealthServiceStatusForOrganization",
        "iam:getAccessKeyLastUsed",
        "iam:getAccountAuthorizationDetails",
        "iam:getAccountPasswordPolicy",
        "iam:getAccountSummary",
        "iam:getContextKeysForCustomPolicy",
        "iam:getContextKeysForPrincipalPolicy",
        "iam:getCredentialReport",
        "iam:getGroup",
        "iam:getGroupPolicy",
        "iam:getInstanceProfile",
        "iam:getLoginProfile",
        "iam:getMFADevice",
        "iam:getOpenIDConnectProvider",
```

```
        "iam:getPolicy",
        "iam:getPolicyVersion",
        "iam:getRole",
        "iam:getRolePolicy",
        "iam:getSAMLProvider",
        "iam:getServerCertificate",
        "iam:getServiceLinkedRoleDeletionStatus",
        "iam:getSSHPublicKey",
        "iam:getUser",
        "iam:getUserPolicy",
        "iam:listAccessKeys",
        "iam:listAccountAliases",
        "iam:listAttachedGroupPolicies",
        "iam:listAttachedRolePolicies",
        "iam:listAttachedUserPolicies",
        "iam:listEntitiesForPolicy",
        "iam:listGroupPolicies",
        "iam:listGroups",
        "iam:listGroupsForUser",
        "iam:listInstanceProfiles",
        "iam:listInstanceProfilesForRole",
        "iam:listMFADevices",
        "iam:listOpenIDConnectProviders",
        "iam:listPolicies",
        "iam:listPolicyVersions",
        "iam:listRolePolicies",
        "iam:listRoles",
        "iam:listSAMLProviders",
        "iam:listServerCertificates",
        "iam:listServiceSpecificCredentials",
        "iam:listSigningCertificates",
        "iam:listSSHPublicKeys",
        "iam:listUserPolicies",
        "iam:listUsers",
        "iam:listVirtualMFADevices",
        "iam:simulateCustomPolicy",
        "iam:simulatePrincipalPolicy",
        "identitystore:describeGroup",
        "identitystore:describeGroupMembership",
        "identitystore:getGroupId",
        "identitystore:getGroupMembershipId",
        "identitystore:getUserId",
        "identitystore:isMemberInGroups",
        "identitystore:listGroupMemberships",
```

```
        "identitystore:listGroupMembershipsForMember",
        "identitystore:listGroups",
        "imagebuilder:getComponent",
        "imagebuilder:getComponentPolicy",
        "imagebuilder:getContainerRecipe",
        "imagebuilder:getContainerRecipePolicy",
        "imagebuilder:getDistributionConfiguration",
        "imagebuilder:getImage",
        "imagebuilder:getImagePipeline",
        "imagebuilder:getImagePolicy",
        "imagebuilder:getImageRecipe",
        "imagebuilder:getImageRecipePolicy",
        "imagebuilder:getInfrastructureConfiguration",
        "imagebuilder:getLifecycleExecution",
        "imagebuilder:getLifecyclePolicy",
        "imagebuilder:getWorkflow",
        "imagebuilder:getWorkflowExecution",
        "imagebuilder:getWorkflowStepExecution",
        "imagebuilder:listComponentBuildVersions",
        "imagebuilder:listComponents",
        "imagebuilder:listContainerRecipes",
        "imagebuilder:listDistributionConfigurations",
        "imagebuilder:listImageBuildVersions",
        "imagebuilder:listImagePipelineImages",
        "imagebuilder:listImagePipelines",
        "imagebuilder:listImageRecipes",
        "imagebuilder:listImages",
        "imagebuilder:listImageScanFindingAggregations",
        "imagebuilder:listInfrastructureConfigurations",
        "imagebuilder:listLifecycleExecutionResources",
        "imagebuilder:listLifecycleExecutions",
        "imagebuilder:listLifecyclePolicies",
        "imagebuilder:listTagsForResource",
        "imagebuilder:listWorkflowBuildVersions",
        "imagebuilder:listWorkflowExecutions",
        "imagebuilder:listWorkflows",
        "imagebuilder:listWaitingWorkflowSteps",
        "imagebuilder:listWorkflowStepExecutions",
        "inspector-scan:scanSbom",
        "inspector:describeAssessmentRuns",
        "inspector:describeAssessmentTargets",
        "inspector:describeAssessmentTemplates",
        "inspector:describeCrossAccountAccessRole",
        "inspector:describeResourceGroups",
```

```
        "inspector:describeRulesPackages",
        "inspector:getTelemetryMetadata",
        "inspector:listAssessmentRunAgents",
        "inspector:listAssessmentRuns",
        "inspector:listAssessmentTargets",
        "inspector:listAssessmentTemplates",
        "inspector:listEventSubscriptions",
        "inspector:listRulesPackages",
        "inspector:listTagsForResource",
        "inspector2:batchGetAccountStatus",
        "inspector2:batchGetFreeTrialInfo",
        "inspector2:describeOrganizationConfiguration",
        "inspector2:getConfiguration",
        "inspector2:getDelegatedAdminAccount",
        "inspector2:getEc2DeepInspectionConfiguration",
        "inspector2:getMember",
        "inspector2:getSbomExport",
        "inspector2:listCisScanConfigurations",
        "inspector2:listCisScanResultsAggregatedByChecks",
        "inspector2:listCisScanResultsAggregatedByTargetResource",
        "inspector2:listCisScans",
        "inspector2:listCoverage",
        "inspector2:listDelegatedAdminAccounts",
        "inspector2:listFilters",
        "inspector2:listFindings",
        "inspector2:listMembers",
        "inspector2:listUsageTotals",
        "internetmonitor:getHealthEvent",
        "internetmonitor:getMonitor",
        "internetmonitor:listHealthEvents",
        "internetmonitor:listMonitors",
        "invoicing:listInvoiceSummaries",
        "iot:describeAuthorizer",
        "iot:describeCACertificate",
        "iot:describeCertificate",
        "iot:describeDefaultAuthorizer",
        "iot:describeDomainConfiguration",
        "iot:describeEndpoint",
        "iot:describeIndex",
        "iot:describeJobExecution",
        "iot:describeThing",
        "iot:describeThingGroup",
        "iot:describeTunnel",
        "iot:getEffectivePolicies",
```

```
        "iot:getIndexingConfiguration",
        "iot:getLoggingOptions",
        "iot:getPolicy",
        "iot:getPolicyVersion",
        "iot:getTopicRule",
        "iot:getV2LoggingOptions",
        "iot:listAttachedPolicies",
        "iot:listAuthorizers",
        "iot:listCACertificates",
        "iot:listCertificates",
        "iot:listCertificatesByCA",
        "iot:listCommandExecutions",
        "iot:listCommands",
        "iot:listDomainConfigurations",
        "iot:listJobExecutionsForJob",
        "iot:listJobExecutionsForThing",
        "iot:listJobs",
        "iot:listNamedShadowsForThing",
        "iot:listOutgoingCertificates",
        "iot:listPackages",
        "iot:listPackageVersions",
        "iot:listPolicies",
        "iot:listPolicyPrincipals",
        "iot:listPolicyVersions",
        "iot:listPrincipalPolicies",
        "iot:listPrincipalThings",
        "iot:listRoleAliases",
        "iot:listTargetsForPolicy",
        "iot:listThingGroups",
        "iot:listThingGroupsForThing",
        "iot:listThingPrincipals",
        "iot:listThingRegistrationTasks",
        "iot:listThings",
        "iot:listThingsInThingGroup",
        "iot:listThingTypes",
        "iot:listTopicRules",
        "iot:listTunnels",
        "iot:listV2LoggingLevels",
        "iotevents:describeDetector",
        "iotevents:describeDetectorModel",
        "iotevents:describeInput",
        "iotevents:describeLoggingOptions",
        "iotevents:listDetectorModels",
        "iotevents:listDetectorModelVersions",
```

```
        "iotevents:listDetectors",
        "iotevents:listInputs",
        "iotfleetwise:getCampaign",
        "iotfleetwise:getDecoderManifest",
        "iotfleetwise:getEncryptionConfiguration",
        "iotfleetwise:getFleet",
        "iotfleetwise:getLoggingOptions",
        "iotfleetwise:getModelManifest",
        "iotfleetwise:getRegisterAccountStatus",
        "iotfleetwise:getSignalCatalog",
        "iotfleetwise:getStateTemplate",
        "iotfleetwise:getVehicle",
        "iotfleetwise:getVehicleStatus",
        "iotfleetwise:listCampaigns",
        "iotfleetwise:listDecoderManifestNetworkInterfaces",
        "iotfleetwise:listDecoderManifests",
        "iotfleetwise:listDecoderManifestSignals",
        "iotfleetwise:listFleets",
        "iotfleetwise:listFleetsForVehicle",
        "iotfleetwise:listModelManifestNodes",
        "iotfleetwise:listModelManifests",
        "iotfleetwise:listSignalCatalogNodes",
        "iotfleetwise:listSignalCatalogs",
        "iotfleetwise:listStateTemplates",
        "iotfleetwise:listVehicles",
        "iotfleetwise:listVehiclesInFleet",
        "iotsitewise:describeAccessPolicy",
        "iotsitewise:describeAsset",
        "iotsitewise:describeAssetModel",
        "iotsitewise:describeAssetProperty",
        "iotsitewise:describeDashboard",
        "iotsitewise:describeGateway",
        "iotsitewise:describeGatewayCapabilityConfiguration",
        "iotsitewise:describeLoggingOptions",
        "iotsitewise:describePortal",
        "iotsitewise:describeProject",
        "iotsitewise:listAccessPolicies",
        "iotsitewise:listAssetModels",
        "iotsitewise:listAssets",
        "iotsitewise:listAssociatedAssets",
        "iotsitewise:listDashboards",
        "iotsitewise:listGateways",
        "iotsitewise:listPortals",
        "iotsitewise:listProjectAssets",
```

```
        "iotsitewise:listProjects",
        "iottwinmaker:getComponentType",
        "iottwinmaker:getEntity",
        "iottwinmaker:getPricingPlan",
        "iottwinmaker:getScene",
        "iottwinmaker:getSyncJob",
        "iottwinmaker:getWorkspace",
        "iottwinmaker:listComponentTypes",
        "iottwinmaker:listEntities",
        "iottwinmaker:listScenes",
        "iottwinmaker:listSyncJobs",
        "iottwinmaker:listSyncResources",
        "iottwinmaker:listWorkspaces",
        "iotwireless:getDestination",
        "iotwireless:getDeviceProfile",
        "iotwireless:getPartnerAccount",
        "iotwireless:getServiceEndpoint",
        "iotwireless:getServiceProfile",
        "iotwireless:getWirelessDevice",
        "iotwireless:getWirelessDeviceStatistics",
        "iotwireless:getWirelessGateway",
        "iotwireless:getWirelessGatewayCertificate",
        "iotwireless:getWirelessGatewayFirmwareInformation",
        "iotwireless:getWirelessGatewayStatistics",
        "iotwireless:getWirelessGatewayTask",
        "iotwireless:getWirelessGatewayTaskDefinition",
        "iotwireless:listDestinations",
        "iotwireless:listDeviceProfiles",
        "iotwireless:listPartnerAccounts",
        "iotwireless:listServiceProfiles",
        "iotwireless:listTagsForResource",
        "iotwireless:listWirelessDevices",
        "iotwireless:listWirelessGateways",
        "iotwireless:listWirelessGatewayTaskDefinitions",
        "ivs:getChannel",
        "ivs:getRecordingConfiguration",
        "ivs:getStream",
        "ivs:getStreamSession",
        "ivs:listChannels",
        "ivs:listPlaybackKeyPairs",
        "ivs:listRecordingConfigurations",
        "ivs:listStreamKeys",
        "ivs:listStreams",
        "ivs:listStreamSessions",
```

```
        "kafka:describeCluster",
        "kafka:describeClusterOperation",
        "kafka:describeClusterOperationV2",
        "kafka:describeClusterV2",
        "kafka:describeConfiguration",
        "kafka:describeConfigurationRevision",
        "kafka:describeReplicator",
        "kafka:describeVpcConnection",
        "kafka:getBootstrapBrokers",
        "kafka:getClusterPolicy",
        "kafka:listClientVpcConnections",
        "kafka:listClusterOperations",
        "kafka:listClusterOperationsV2",
        "kafka:listClusters",
        "kafka:listClustersV2",
        "kafka:listConfigurationRevisions",
        "kafka:listConfigurations",
        "kafka:listNodes",
        "kafka:listReplicators",
        "kafka:listScramSecrets",
        "kafka:listVpcConnections",
        "kafkaconnect:describeConnector",
        "kafkaconnect:describeCustomPlugin",
        "kafkaconnect:describeWorkerConfiguration",
        "kafkaconnect:listConnectors",
        "kafkaconnect:listCustomPlugins",
        "kafkaconnect:listWorkerConfigurations",
        "kendra:describeDataSource",
        "kendra:describeFaq",
        "kendra:describeIndex",
        "kendra:listDataSources",
        "kendra:listFaqs",
        "kendra:listIndices",
        "kinesis:describeStream",
        "kinesis:describeStreamConsumer",
        "kinesis:describeStreamSummary",
        "kinesis:listShards",
        "kinesis:listStreamConsumers",
        "kinesis:listStreams",
        "kinesis:listTagsForStream",
        "kinesisanalytics:describeApplication",
        "kinesisanalytics:describeApplicationOperation",
        "kinesisanalytics:describeApplicationSnapshot",
        "kinesisanalytics:listApplicationOperations",
```

```
        "kinesisanalytics:listApplications",
        "kinesisanalytics:listApplicationSnapshots",
        "kinesisanalytics:listApplicationVersions",
        "kinesisvideo:describeImageGenerationConfiguration",
        "kinesisvideo:describeNotificationConfiguration",
        "kinesisvideo:describeSignalingChannel",
        "kinesisvideo:describeStream",
        "kinesisvideo:getDataEndpoint",
        "kinesisvideo:getIceServerConfig",
        "kinesisvideo:getSignalingChannelEndpoint",
        "kinesisvideo:listSignalingChannels",
        "kinesisvideo:listStreams",
        "kms:describeKey",
        "kms:getKeyPolicy",
        "kms:getKeyRotationStatus",
        "kms:listAliases",
        "kms:listGrants",
        "kms:listKeyPolicies",
        "kms:listKeys",
        "kms:listResourceTags",
        "kms:listRetirableGrants",
        "lakeformation:describeLakeFormationIdentityCenterConfiguration",
        "lakeformation:describeResource",
        "lakeformation:describeTransaction",
        "lakeformation:getDataLakePrincipal",
        "lakeformation:getDataLakeSettings",
        "lakeformation:getEffectivePermissionsForPath",
        "lakeformation:getLFTag",
        "lakeformation:getLFTagExpression",
        "lakeformation:getQueryState",
        "lakeformation:getQueryStatistics",
        "lakeformation:getResourceLFTags",
        "lakeformation:listLFTagExpressions",
        "lakeformation:listLFTags",
        "lakeformation:listLakeFormationOptIns",
        "lakeformation:listPermissions",
        "lakeformation:listResources",
        "lakeformation:searchDatabasesByLFTags",
        "lakeformation:searchTablesByLFTags",
        "lambda:getAccountSettings",
        "lambda:getAlias",
        "lambda:getCodeSigningConfig",
        "lambda:getEventSourceMapping",
        "lambda:getFunction",
```

```
        "lambda:getFunctionCodeSigningConfig",
        "lambda:getFunctionConcurrency",
        "lambda:getFunctionConfiguration",
        "lambda:getFunctionEventInvokeConfig",
        "lambda:getFunctionRecursionConfig",
        "lambda:getFunctionUrlConfig",
        "lambda:getLayerVersion",
        "lambda:getLayerVersionPolicy",
        "lambda:getPolicy",
        "lambda:getProvisionedConcurrencyConfig",
        "lambda:getRuntimeManagementConfig",
        "lambda:listAliases",
        "lambda:listCodeSigningConfigs",
        "lambda:listEventSourceMappings",
        "lambda:listFunctionEventInvokeConfigs",
        "lambda:listFunctions",
        "lambda:listFunctionsByCodeSigningConfig",
        "lambda:listFunctionUrlConfigs",
        "lambda:listLayers",
        "lambda:listLayerVersions",
        "lambda:listProvisionedConcurrencyConfigs",
        "lambda:listTags",
        "lambda:listVersionsByFunction",
        "launchwizard:describeProvisionedApp",
        "launchwizard:describeProvisioningEvents",
        "launchwizard:listDeploymentEvents",
        "launchwizard:listDeployments",
        "launchwizard:listProvisionedApps",
        "lex:describeBot",
        "lex:describeBotAlias",
        "lex:describeBotLocale",
        "lex:describeBotRecommendation",
        "lex:describeBotVersion",
        "lex:describeCustomVocabularyMetadata",
        "lex:describeExport",
        "lex:describeImport",
        "lex:describeIntent",
        "lex:describeResourcePolicy",
        "lex:describeSlot",
        "lex:describeSlotType",
        "lex:getBot",
        "lex:getBotAlias",
        "lex:getBotAliases",
        "lex:getBotChannelAssociation",
```

```
        "lex:getBotChannelAssociations",
        "lex:getBots",
        "lex:getBotVersions",
        "lex:getBuiltinIntent",
        "lex:getBuiltinIntents",
        "lex:getBuiltinSlotTypes",
        "lex:getIntent",
        "lex:getIntents",
        "lex:getIntentVersions",
        "lex:getSlotType",
        "lex:getSlotTypes",
        "lex:getSlotTypeVersions",
        "lex:listBotAliases",
        "lex:listBotLocales",
        "lex:listBotRecommendations",
        "lex:listBots",
        "lex:listBotVersions",
        "lex:listExports",
        "lex:listImports",
        "lex:listIntents",
        "lex:listRecommendedIntents",
        "lex:listSlots",
        "lex:listSlotTypes",
        "license-manager:getLicenseConfiguration",
        "license-manager:getServiceSettings",
        "license-manager:listAssociationsForLicenseConfiguration",
        "license-manager:listFailuresForLicenseConfigurationOperations",
        "license-manager:listLicenseConfigurations",
        "license-manager:listLicenseSpecificationsForResource",
        "license-manager:listResourceInventory",
        "license-manager:listUsageForLicenseConfiguration",
        "lightsail:getActiveNames",
        "lightsail:getAlarms",
        "lightsail:getAutoSnapshots",
        "lightsail:getBlueprints",
        "lightsail:getBucketBundles",
        "lightsail:getBucketMetricData",
        "lightsail:getBuckets",
        "lightsail:getBundles",
        "lightsail:getCertificates",
        "lightsail:getContainerImages",
        "lightsail:getContainerServiceDeployments",
        "lightsail:getContainerServiceMetricData",
        "lightsail:getContainerServicePowers",
```

```
        "lightsail:getContainerServices",
        "lightsail:getDisk",
        "lightsail:getDisks",
        "lightsail:getDiskSnapshot",
        "lightsail:getDiskSnapshots",
        "lightsail:getDistributionBundles",
        "lightsail:getDistributionMetricData",
        "lightsail:getDistributions",
        "lightsail:getDomain",
        "lightsail:getDomains",
        "lightsail:getExportSnapshotRecords",
        "lightsail:getInstance",
        "lightsail:getInstanceMetricData",
        "lightsail:getInstancePortStates",
        "lightsail:getInstances",
        "lightsail:getInstanceSnapshot",
        "lightsail:getInstanceSnapshots",
        "lightsail:getInstanceState",
        "lightsail:getKeyPair",
        "lightsail:getKeyPairs",
        "lightsail:getLoadBalancer",
        "lightsail:getLoadBalancerMetricData",
        "lightsail:getLoadBalancers",
        "lightsail:getLoadBalancerTlsCertificates",
        "lightsail:getOperation",
        "lightsail:getOperations",
        "lightsail:getOperationsForResource",
        "lightsail:getRegions",
        "lightsail:getRelationalDatabase",
        "lightsail:getRelationalDatabaseMetricData",
        "lightsail:getRelationalDatabases",
        "lightsail:getRelationalDatabaseSnapshot",
        "lightsail:getRelationalDatabaseSnapshots",
        "lightsail:getStaticIp",
        "lightsail:getStaticIps",
        "lightsail:isVpcPeered",
        "logs:describeAccountPolicies",
        "logs:describeDeliveries",
        "logs:describeDeliveryDestinations",
        "logs:describeDeliverySources",
        "logs:describeDestinations",
        "logs:describeExportTasks",
        "logs:describeFieldIndexes",
        "logs:describeIndexPolicies",
```

```
        "logs:describeLogGroups",
        "logs:describeLogStreams",
        "logs:describeMetricFilters",
        "logs:describeQueries",
        "logs:describeQueryDefinitions",
        "logs:describeResourcePolicies",
        "logs:describeSubscriptionFilters",
        "logs:getDataProtectionPolicy",
        "logs:getDelivery",
        "logs:getDeliveryDestination",
        "logs:getDeliveryDestinationPolicy",
        "logs:getDeliverySource",
        "logs:getIntegration",
        "logs:getLogAnomalyDetector",
        "logs:getLogDelivery",
        "logs:getLogGroupFields",
        "logs:getTransformer",
        "logs:listAnomalies",
        "logs:listIntegrations",
        "logs:listLogAnomalyDetectors",
        "logs:listLogDeliveries",
        "logs:listLogGroupsForQuery",
        "logs:testMetricFilter",
        "lookoutequipment:describeDataIngestionJob",
        "lookoutequipment:describeDataset",
        "lookoutequipment:describeInferenceScheduler",
        "lookoutequipment:describeModel",
        "lookoutequipment:listDataIngestionJobs",
        "lookoutequipment:listDatasets",
        "lookoutequipment:listInferenceExecutions",
        "lookoutequipment:listInferenceSchedulers",
        "lookoutequipment:listModels",
        "lookoutmetrics:describeAlert",
        "lookoutmetrics:describeAnomalyDetectionExecutions",
        "lookoutmetrics:describeAnomalyDetector",
        "lookoutmetrics:describeMetricSet",
        "lookoutmetrics:getAnomalyGroup",
        "lookoutmetrics:getDataQualityMetrics",
        "lookoutmetrics:getFeedback",
        "lookoutmetrics:getSampleData",
        "lookoutmetrics:listAlerts",
        "lookoutmetrics:listAnomalyDetectors",
        "lookoutmetrics:listAnomalyGroupSummaries",
        "lookoutmetrics:listAnomalyGroupTimeSeries",
```

```
        "lookoutmetrics:listMetricSets",
        "lookoutmetrics:listTagsForResource",
        "m2:getApplication",
        "m2:getApplicationVersion",
        "m2:getBatchJobExecution",
        "m2:getDataSetDetails",
        "m2:getDataSetImportTask",
        "m2:getDeployment",
        "m2:getEnvironment",
        "m2:listApplications",
        "m2:listApplicationVersions",
        "m2:listBatchJobDefinitions",
        "m2:listBatchJobExecutions",
        "m2:listDataSetImportHistory",
        "m2:listDataSets",
        "m2:listDeployments",
        "m2:listEngineVersions",
        "m2:listEnvironments",
        "machinelearning:describeBatchPredictions",
        "machinelearning:describeDataSources",
        "machinelearning:describeEvaluations",
        "machinelearning:describeMLModels",
        "machinelearning:getBatchPrediction",
        "machinelearning:getDataSource",
        "machinelearning:getEvaluation",
        "machinelearning:getMLModel",
        "macie2:getClassificationExportConfiguration",
        "macie2:getCustomDataIdentifier",
        "macie2:getFindings",
        "macie2:getFindingStatistics",
        "macie2:listClassificationJobs",
        "macie2:listCustomDataIdentifiers",
        "macie2:listFindings",
        "managedblockchain:getMember",
        "managedblockchain:getNetwork",
        "managedblockchain:getNode",
        "managedblockchain:listMembers",
        "managedblockchain:listNetworks",
        "managedblockchain:listNodes",
        "mediaconnect:describeFlow",
        "mediaconnect:listEntitlements",
        "mediaconnect:listFlows",
        "mediaconvert:describeEndpoints",
        "mediaconvert:getJob",
```

```
        "mediaconvert:getJobTemplate",
        "mediaconvert:getPreset",
        "mediaconvert:getQueue",
        "mediaconvert:listJobs",
        "mediaconvert:listJobTemplates",
        "medialive:describeChannel",
        "medialive:describeInput",
        "medialive:describeInputDevice",
        "medialive:describeInputSecurityGroup",
        "medialive:describeMultiplex",
        "medialive:describeOffering",
        "medialive:describeReservation",
        "medialive:describeSchedule",
        "medialive:getCloudWatchAlarmTemplate",
        "medialive:getCloudWatchAlarmTemplateGroup",
        "medialive:getEventBridgeRuleTemplate",
        "medialive:getEventBridgeRuleTemplateGroup",
        "medialive:getSignalMap",
        "medialive:listChannels",
        "medialive:listCloudWatchAlarmTemplateGroups",
        "medialive:listCloudWatchAlarmTemplates",
        "medialive:listEventBridgeRuleTemplateGroups",
        "medialive:listEventBridgeRuleTemplates",
        "medialive:listInputDevices",
        "medialive:listInputs",
        "medialive:listInputSecurityGroups",
        "medialive:listMultiplexes",
        "medialive:listOfferings",
        "medialive:listReservations",
        "medialive:listSignalMaps",
        "mediapackage:describeChannel",
        "mediapackage:describeOriginEndpoint",
        "mediapackage:listChannels",
        "mediapackage:listOriginEndpoints",
        "mediastore:describeContainer",
        "mediastore:getContainerPolicy",
        "mediastore:getCorsPolicy",
        "mediastore:listContainers",
        "mediatailor:getPlaybackConfiguration",
        "mediatailor:listPlaybackConfigurations",
        "medical-imaging:getDatastore",
        "medical-imaging:listDatastores",
        "mgn:describeJobLogItems",
        "mgn:describeJobs",
```

```
        "mgn:describeLaunchConfigurationTemplates",
        "mgn:describeReplicationConfigurationTemplates",
        "mgn:describeSourceServers",
        "mgn:describeVcenterClients",
        "mgn:getLaunchConfiguration",
        "mgn:getReplicationConfiguration",
        "mgn:listApplications",
        "mgn:listSourceServerActions",
        "mgn:listTemplateActions",
        "mgn:listWaves",
        "mobiletargeting:getAdmChannel",
        "mobiletargeting:getApnsChannel",
        "mobiletargeting:getApnsSandboxChannel",
        "mobiletargeting:getApnsVoipChannel",
        "mobiletargeting:getApnsVoipSandboxChannel",
        "mobiletargeting:getApp",
        "mobiletargeting:getApplicationSettings",
        "mobiletargeting:getApps",
        "mobiletargeting:getBaiduChannel",
        "mobiletargeting:getCampaign",
        "mobiletargeting:getCampaignActivities",
        "mobiletargeting:getCampaigns",
        "mobiletargeting:getCampaignVersion",
        "mobiletargeting:getCampaignVersions",
        "mobiletargeting:getEmailChannel",
        "mobiletargeting:getEndpoint",
        "mobiletargeting:getEventStream",
        "mobiletargeting:getExportJob",
        "mobiletargeting:getExportJobs",
        "mobiletargeting:getGcmChannel",
        "mobiletargeting:getImportJob",
        "mobiletargeting:getImportJobs",
        "mobiletargeting:getJourney",
        "mobiletargeting:getJourneyExecutionActivityMetrics",
        "mobiletargeting:getJourneyExecutionMetrics",
        "mobiletargeting:getJourneyRunExecutionActivityMetrics",
        "mobiletargeting:getJourneyRunExecutionMetrics",
        "mobiletargeting:getJourneyRuns",
        "mobiletargeting:getSegment",
        "mobiletargeting:getSegmentImportJobs",
        "mobiletargeting:getSegments",
        "mobiletargeting:getSegmentVersion",
        "mobiletargeting:getSegmentVersions",
        "mobiletargeting:getSmsChannel",
```

```
        "mobiletargeting:listJourneys",
        "mobiletargeting:phoneNumberValidate",
        "mq:describeBroker",
        "mq:describeConfiguration",
        "mq:describeConfigurationRevision",
        "mq:describeUser",
        "mq:listBrokers",
        "mq:listConfigurationRevisions",
        "mq:listConfigurations",
        "mq:listUsers",
        "network-firewall:describeFirewall",
        "network-firewall:describeFirewallPolicy",
        "network-firewall:describeFlowOperation",
        "network-firewall:describeLoggingConfiguration",
        "network-firewall:describeResourcePolicy",
        "network-firewall:describeRuleGroup",
        "network-firewall:describeRuleGroupMetadata",
        "network-firewall:describeTlsInspectionConfiguration",
        "network-firewall:describeVpcEndpointAssociation",
        "network-firewall:listAnalysisReports",
        "network-firewall:listFirewallPolicies",
        "network-firewall:listFirewalls",
        "network-firewall:listFlowOperationResults",
        "network-firewall:listFlowOperations",
        "network-firewall:listRuleGroups",
        "network-firewall:listTlsInspectionConfigurations",
        "network-firewall:listVpcEndpointAssociations",
        "networkflowmonitor:getMonitor",
        "networkflowmonitor:getScope",
        "networkflowmonitor:listMonitors",
        "networkflowmonitor:listScopes",
        "networkmanager:describeGlobalNetworks",
        "networkmanager:getConnectAttachment",
        "networkmanager:getConnections",
        "networkmanager:getConnectPeer",
        "networkmanager:getConnectPeerAssociations",
        "networkmanager:getCoreNetwork",
        "networkmanager:getCoreNetworkChangeEvents",
        "networkmanager:getCoreNetworkChangeSet",
        "networkmanager:getCoreNetworkPolicy",
        "networkmanager:getCustomerGatewayAssociations",
        "networkmanager:getDevices",
        "networkmanager:getDirectConnectGatewayAttachment",
        "networkmanager:getLinkAssociations",
```

```
        "networkmanager:getLinks",
        "networkmanager:getNetworkResourceCounts",
        "networkmanager:getNetworkResourceRelationships",
        "networkmanager:getNetworkResources",
        "networkmanager:getNetworkRoutes",
        "networkmanager:getNetworkTelemetry",
        "networkmanager:getResourcePolicy",
        "networkmanager:getRouteAnalysis",
        "networkmanager:getSites",
        "networkmanager:getSiteToSiteVpnAttachment",
        "networkmanager:getTransitGatewayConnectPeerAssociations",
        "networkmanager:getTransitGatewayPeering",
        "networkmanager:getTransitGatewayRegistrations",
        "networkmanager:getTransitGatewayRouteTableAttachment",
        "networkmanager:getVpcAttachment",
        "networkmanager:listAttachments",
        "networkmanager:listConnectPeers",
        "networkmanager:listCoreNetworkPolicyVersions",
        "networkmanager:listCoreNetworks",
        "networkmanager:listOrganizationServiceAccessStatus",
        "networkmanager:listPeerings",
        "networkmanager:listTagsForResource",
        "networkmonitor:getMonitor",
        "networkmonitor:getProbe",
        "networkmonitor:listMonitors",
        "notifications-contacts:getEmailContact",
        "notifications-contacts:listEmailContacts",
        "notifications:getEventRule",
        "notifications:getNotificationConfiguration",
        "notifications:getNotificationEvent",
        "notifications:listChannels",
        "notifications:listEventRules",
        "notifications:listNotificationConfigurations",
        "notifications:listNotificationEvents",
        "notifications:listNotificationHubs"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSSupportActionsGroup3",
      "Action" : [
```

```
        "oam:getLink",
        "oam:getSink",
        "oam:getSinkPolicy",
        "oam:listAttachedLinks",
        "oam:listLinks",
        "oam:listSinks",
        "observabilityadmin:getTelemetryEvaluationStatus",
        "observabilityadmin:getTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:listResourceTelemetry",
        "observabilityadmin:listResourceTelemetryForOrganization",
        "odb:getOciOnboardingStatus",
        "odb:getOdbNetwork",
        "odb:getOdbPeeringConnection",
        "odb:listOdbNetworks",
        "odb:listOdbPeeringConnections",
        "omics:getAnnotationImportJob",
        "omics:getAnnotationStore",
        "omics:getAnnotationStoreVersion",
        "omics:getReadSetActivationJob",
        "omics:getReadSetExportJob",
        "omics:getReadSetImportJob",
        "omics:getReadSetMetadata",
        "omics:getReference",
        "omics:getReferenceImportJob",
        "omics:getReferenceMetadata",
        "omics:getReferenceStore",
        "omics:getRun",
        "omics:getRunCache",
        "omics:getRunGroup",
        "omics:getRunTask",
        "omics:getSequenceStore",
        "omics:getShare",
        "omics:getVariantImportJob",
        "omics:getVariantStore",
        "omics:getWorkflow",
        "omics:getWorkflowVersion",
        "omics:listAnnotationImportJobs",
        "omics:listAnnotationStores",
        "omics:listAnnotationStoreVersions",
        "omics:listMultipartReadSetUploads",
        "omics:listReadSetActivationJobs",
        "omics:listReadSetExportJobs",
        "omics:listReadSetImportJobs",
        "omics:listReadSets",
```

```
        "omics:listReadSetUploadParts",
        "omics:listReferenceImportJobs",
        "omics:listReferences",
        "omics:listReferenceStores",
        "omics:listRunCaches",
        "omics:listRunGroups",
        "omics:listRuns",
        "omics:listRunTasks",
        "omics:listSequenceStores",
        "omics:listShares",
        "omics:listVariantImportJobs",
        "omics:listVariantStores",
        "omics:listWorkflows",
        "omics:listWorkflowVersions",
        "opsworks-cm:describeAccountAttributes",
        "opsworks-cm:describeBackups",
        "opsworks-cm:describeEvents",
        "opsworks-cm:describeNodeAssociationStatus",
        "opsworks-cm:describeServers",
        "opsworks:describeAgentVersions",
        "opsworks:describeApps",
        "opsworks:describeCommands",
        "opsworks:describeDeployments",
        "opsworks:describeEcsClusters",
        "opsworks:describeElasticIps",
        "opsworks:describeElasticLoadBalancers",
        "opsworks:describeInstances",
        "opsworks:describeLayers",
        "opsworks:describeLoadBasedAutoScaling",
        "opsworks:describeMyUserProfile",
        "opsworks:describePermissions",
        "opsworks:describeRaidArrays",
        "opsworks:describeRdsDbInstances",
        "opsworks:describeServiceErrors",
        "opsworks:describeStackProvisioningParameters",
        "opsworks:describeStacks",
        "opsworks:describeStackSummary",
        "opsworks:describeTimeBasedAutoScaling",
        "opsworks:describeUserProfiles",
        "opsworks:describeVolumes",
        "opsworks:getHostnameSuggestion",
        "organizations:describeAccount",
        "organizations:describeCreateAccountStatus",
        "organizations:describeEffectivePolicy",
```

```
        "organizations:describeHandshake",
        "organizations:describeOrganization",
        "organizations:describeOrganizationalUnit",
        "organizations:describePolicy",
        "organizations:describeResourcePolicy",
        "organizations:listAccounts",
        "organizations:listAccountsForParent",
        "organizations:listAWSServiceAccessForOrganization",
        "organizations:listChildren",
        "organizations:listCreateAccountStatus",
        "organizations:listDelegatedAdministrators",
        "organizations:listDelegatedServicesForAccount",
        "organizations:listHandshakesForAccount",
        "organizations:listHandshakesForOrganization",
        "organizations:listOrganizationalUnitsForParent",
        "organizations:listParents",
        "organizations:listPolicies",
        "organizations:listPoliciesForTarget",
        "organizations:listRoots",
        "organizations:listTagsForResource",
        "organizations:listTargetsForPolicy",
        "osis:getPipeline",
        "osis:getPipelineBlueprint",
        "osis:getPipelineChangeProgress",
        "osis:listPipelineBlueprints",
        "osis:listPipelines",
        "osis:validatePipeline",
        "outposts:getCapacityTask",
        "outposts:getCatalogItem",
        "outposts:getConnection",
        "outposts:getOrder",
        "outposts:getOutpost",
        "outposts:getOutpostInstanceTypes",
        "outposts:getOutpostSupportedInstanceTypes",
        "outposts:getSite",
        "outposts:listAssets",
        "outposts:listAssetInstances",
        "outposts:listBlockingInstancesForCapacityTask",
        "outposts:listCapacityTasks",
        "outposts:listCatalogItems",
        "outposts:listOrders",
        "outposts:listOutposts",
        "outposts:listSites",
        "pcs:getCluster",
```

```
        "pcs:getComputeNodeGroup",
        "pcs:getQueue",
        "pcs:listClusters",
        "pcs:listComputeNodeGroups",
        "pcs:listQueues",
        "personalize:describeAlgorithm",
        "personalize:describeBatchInferenceJob",
        "personalize:describeBatchSegmentJob",
        "personalize:describeCampaign",
        "personalize:describeDataset",
        "personalize:describeDatasetExportJob",
        "personalize:describeDatasetGroup",
        "personalize:describeDatasetImportJob",
        "personalize:describeEventTracker",
        "personalize:describeFeatureTransformation",
        "personalize:describeFilter",
        "personalize:describeRecipe",
        "personalize:describeRecommender",
        "personalize:describeSchema",
        "personalize:describeSolution",
        "personalize:describeSolutionVersion",
        "personalize:getPersonalizedRanking",
        "personalize:getRecommendations",
        "personalize:getSolutionMetrics",
        "personalize:listBatchInferenceJobs",
        "personalize:listBatchSegmentJobs",
        "personalize:listCampaigns",
        "personalize:listDatasetExportJobs",
        "personalize:listDatasetGroups",
        "personalize:listDatasetImportJobs",
        "personalize:listDatasets",
        "personalize:listEventTrackers",
        "personalize:listRecipes",
        "personalize:listRecommenders",
        "personalize:listSchemas",
        "personalize:listSolutions",
        "personalize:listSolutionVersions",
        "pipes:describePipe",
        "pipes:listPipes",
        "pipes:listTagsForResource",
        "polly:describeVoices",
        "polly:getLexicon",
        "polly:listLexicons",
        "pricing:describeServices",
```

```
        "pricing:getAttributeValues",
        "pricing:getProducts",
        "private-networks:getDeviceIdentifier",
        "private-networks:getNetwork",
        "private-networks:getNetworkResource",
        "private-networks:listDeviceIdentifiers",
        "private-networks:listNetworkResources",
        "private-networks:listNetworks",
        "qbusiness:getApplication",
        "qbusiness:getDataSource",
        "qbusiness:getIndex",
        "qbusiness:getRetriever",
        "qbusiness:getWebExperience",
        "qbusiness:listApplications",
        "qbusiness:listDataSources",
        "qbusiness:listDataSourceSyncJobs",
        "qbusiness:listIndices",
        "qbusiness:listRetrievers",
        "qbusiness:listWebExperiences",
        "quicksight:describeAccountCustomization",
        "quicksight:describeAccountSettings",
        "quicksight:describeAccountSubscription",
        "quicksight:describeAnalysis",
        "quicksight:describeAnalysisPermissions",
        "quicksight:describeDashboard",
        "quicksight:describeDashboardPermissions",
        "quicksight:describeDataSet",
        "quicksight:describeDataSetPermissions",
        "quicksight:describeDataSetRefreshProperties",
        "quicksight:describeDataSource",
        "quicksight:describeDataSourcePermissions",
        "quicksight:describeFolder",
        "quicksight:describeFolderPermissions",
        "quicksight:describeFolderResolvedPermissions",
        "quicksight:describeGroup",
        "quicksight:describeGroupMembership",
        "quicksight:describeIAMPolicyAssignment",
        "quicksight:describeIngestion",
        "quicksight:describeIpRestriction",
        "quicksight:describeNamespace",
        "quicksight:describeRefreshSchedule",
        "quicksight:describeTemplate",
        "quicksight:describeTemplateAlias",
        "quicksight:describeTemplatePermissions",
```

```
        "quicksight:describeTheme",
        "quicksight:describeThemeAlias",
        "quicksight:describeThemePermissions",
        "quicksight:describeTopic",
        "quicksight:describeTopicPermissions",
        "quicksight:describeTopicRefresh",
        "quicksight:describeTopicRefreshSchedule",
        "quicksight:describeUser",
        "quicksight:describeVPCConnection",
        "quicksight:listAnalyses",
        "quicksight:listDashboards",
        "quicksight:listDashboardVersions",
        "quicksight:listDataSets",
        "quicksight:listDataSources",
        "quicksight:listFolderMembers",
        "quicksight:listFolders",
        "quicksight:listGroupMemberships",
        "quicksight:listGroups",
        "quicksight:listIAMPolicyAssignments",
        "quicksight:listIAMPolicyAssignmentsForUser",
        "quicksight:listIngestions",
        "quicksight:listNamespaces",
        "quicksight:listRefreshSchedules",
        "quicksight:listTemplateAliases",
        "quicksight:listTemplates",
        "quicksight:listTemplateVersions",
        "quicksight:listThemeAliases",
        "quicksight:listThemes",
        "quicksight:listThemeVersions",
        "quicksight:listTopicRefreshSchedules",
        "quicksight:listTopics",
        "quicksight:listUserGroups",
        "quicksight:listUsers",
        "quicksight:listVPCConnections",
        "quicksight:searchAnalyses",
        "quicksight:searchDashboards",
        "quicksight:searchDataSets",
        "quicksight:searchDataSources",
        "quicksight:searchFolders",
        "quicksight:searchGroups",
        "ram:getPermission",
        "ram:getResourceShareAssociations",
        "ram:getResourceShareInvitations",
        "ram:getResourceShares",
```

```
        "ram:listPendingInvitationResources",
        "ram:listPrincipals",
        "ram:listResources",
        "ram:listResourceSharePermissions",
        "rbin:getRule",
        "rbin:listRules",
        "rds:describeAccountAttributes",
        "rds:describeBlueGreenDeployments",
        "rds:describeCertificates",
        "rds:describeDBClusterEndpoints",
        "rds:describeDBClusterParameterGroups",
        "rds:describeDBClusterParameters",
        "rds:describeDBClusters",
        "rds:describeDBClusterSnapshots",
        "rds:describeDBEngineVersions",
        "rds:describeDBInstanceAutomatedBackups",
        "rds:describeDBInstances",
        "rds:describeDBLogFiles",
        "rds:describeDBParameterGroups",
        "rds:describeDBParameters",
        "rds:describeDBSecurityGroups",
        "rds:describeDBSnapshotAttributes",
        "rds:describeDBSnapshots",
        "rds:describeDBSubnetGroups",
        "rds:describeEngineDefaultClusterParameters",
        "rds:describeEngineDefaultParameters",
        "rds:describeEventCategories",
        "rds:describeEvents",
        "rds:describeEventSubscriptions",
        "rds:describeExportTasks",
        "rds:describeGlobalClusters",
        "rds:describeIntegrations",
        "rds:describeOptionGroupOptions",
        "rds:describeOptionGroups",
        "rds:describeOrderableDBInstanceOptions",
        "rds:describePendingMaintenanceActions",
        "rds:describeReservedDBInstances",
        "rds:describeReservedDBInstancesOfferings",
        "rds:describeSourceRegions",
        "rds:describeValidDBInstanceModifications",
        "rds:listTagsForResource",
        "redshift-data:describeStatement",
        "redshift-data:listStatements",
        "redshift-serverless:getCustomDomainAssociation",
```

```
        "redshift-serverless:getEndpointAccess",
        "redshift-serverless:getNamespace",
        "redshift-serverless:getRecoveryPoint",
        "redshift-serverless:getScheduledAction",
        "redshift-serverless:getSnapshot",
        "redshift-serverless:getTableRestoreStatus",
        "redshift-serverless:getUsageLimit",
        "redshift-serverless:getWorkgroup",
        "redshift-serverless:listCustomDomainAssociations",
        "redshift-serverless:listEndpointAccess",
        "redshift-serverless:listNamespaces",
        "redshift-serverless:listRecoveryPoints",
        "redshift-serverless:listSnapshotCopyConfigurations",
        "redshift-serverless:listSnapshots",
        "redshift-serverless:listTableRestoreStatus",
        "redshift-serverless:listUsageLimits",
        "redshift-serverless:listWorkgroups",
        "redshift:describeClusterDbRevisions",
        "redshift:describeClusterParameterGroups",
        "redshift:describeClusterParameters",
        "redshift:describeClusters",
        "redshift:describeClusterSecurityGroups",
        "redshift:describeClusterSnapshots",
        "redshift:describeClusterSubnetGroups",
        "redshift:describeClusterTracks",
        "redshift:describeClusterVersions",
        "redshift:describeCustomDomainAssociations",
        "redshift:describeDataShares",
        "redshift:describeDataSharesForConsumer",
        "redshift:describeDataSharesForProducer",
        "redshift:describeDefaultClusterParameters",
        "redshift:describeEndpointAccess",
        "redshift:describeEndpointAuthorization",
        "redshift:describeEventCategories",
        "redshift:describeEvents",
        "redshift:describeEventSubscriptions",
        "redshift:describeHsmClientCertificates",
        "redshift:describeHsmConfigurations",
        "redshift:describeInboundIntegrations",
        "redshift:describeLoggingStatus",
        "redshift:describeNodeConfigurationOptions",
        "redshift:describeOrderableClusterOptions",
        "redshift:describeRedshiftIdcApplications",
        "redshift:describeReservedNodeOfferings",
```

```
        "redshift:describeReservedNodes",
        "redshift:describeResize",
        "redshift:describeSnapshotCopyGrants",
        "redshift:describeSnapshotSchedules",
        "redshift:describeStorage",
        "redshift:describeTableRestoreStatus",
        "redshift:describeTags",
        "redshift:describeUsageLimits",
        "rekognition:listCollections",
        "rekognition:listFaces",
        "resiliencehub:describeApp",
        "resiliencehub:describeAppAssessment",
        "resiliencehub:describeAppVersion",
        "resiliencehub:describeAppVersionAppComponent",
        "resiliencehub:describeAppVersionResource",
        "resiliencehub:describeAppVersionResourcesResolutionStatus",
        "resiliencehub:describeAppVersionTemplate",
        "resiliencehub:describeDraftAppVersionResourcesImportStatus",
        "resiliencehub:describeResiliencyPolicy",
        "resiliencehub:describeResourceGroupingRecommendationTask",
        "resiliencehub:listAlarmRecommendations",
        "resiliencehub:listAppAssessmentComplianceDrifts",
        "resiliencehub:listAppAssessmentResourceDrifts",
        "resiliencehub:listAppAssessments",
        "resiliencehub:listAppComponentCompliances",
        "resiliencehub:listAppComponentRecommendations",
        "resiliencehub:listAppInputSources",
        "resiliencehub:listApps",
        "resiliencehub:listAppVersionAppComponents",
        "resiliencehub:listAppVersionResourceMappings",
        "resiliencehub:listAppVersionResources",
        "resiliencehub:listAppVersions",
        "resiliencehub:listRecommendationTemplates",
        "resiliencehub:listResiliencyPolicies",
        "resiliencehub:listResourceGroupingRecommendations",
        "resiliencehub:listSopRecommendations",
        "resiliencehub:listSuggestedResiliencyPolicies",
        "resiliencehub:listTestRecommendations",
        "resiliencehub:listUnsupportedAppVersionResources",
        "resource-explorer-2:getAccountLevelServiceConfiguration",
        "resource-explorer-2:getIndex",
        "resource-explorer-2:getView",
        "resource-explorer-2:listIndexes",
        "resource-explorer-2:listViews",
```

```
        "resource-explorer-2:search",
        "resource-groups:getGroup",
        "resource-groups:getGroupQuery",
        "resource-groups:getTags",
        "resource-groups:listGroupResources",
        "resource-groups:listGroups",
        "resource-groups:searchResources",
        "robomaker:batchDescribeSimulationJob",
        "robomaker:describeDeploymentJob",
        "robomaker:describeFleet",
        "robomaker:describeRobot",
        "robomaker:describeRobotApplication",
        "robomaker:describeSimulationApplication",
        "robomaker:describeSimulationJob",
        "robomaker:listDeploymentJobs",
        "robomaker:listFleets",
        "robomaker:listRobotApplications",
        "robomaker:listRobots",
        "robomaker:listSimulationApplications",
        "robomaker:listSimulationJobs",
        "rolesanywhere:getProfile",
        "rolesanywhere:getTrustAnchor",
        "rolesanywhere:listProfiles",
        "rolesanywhere:listTrustAnchors",
        "route53-recovery-cluster:getRoutingControlState",
        "route53-recovery-cluster:listRoutingControls",
        "route53-recovery-control-config:describeControlPanel",
        "route53-recovery-control-config:describeRoutingControl",
        "route53-recovery-control-config:describeSafetyRule",
        "route53-recovery-control-config:listControlPanels",
        "route53-recovery-control-config:listRoutingControls",
        "route53-recovery-control-config:listSafetyRules",
        "route53-recovery-readiness:getCell",
        "route53-recovery-readiness:getCellReadinessSummary",
        "route53-recovery-readiness:getReadinessCheck",
        "route53-recovery-readiness:getReadinessCheckResourceStatus",
        "route53-recovery-readiness:getReadinessCheckStatus",
        "route53-recovery-readiness:getRecoveryGroup",
        "route53-recovery-readiness:getRecoveryGroupReadinessSummary",
        "route53-recovery-readiness:listCells",
        "route53-recovery-readiness:listReadinessChecks",
        "route53-recovery-readiness:listRecoveryGroups",
        "route53-recovery-readiness:listResourceSets",
        "route53:getAccountLimit",
```

```
        "route53:getChange",
        "route53:getCheckerIpRanges",
        "route53:getDNSSEC",
        "route53:getGeoLocation",
        "route53:getHealthCheck",
        "route53:getHealthCheckCount",
        "route53:getHealthCheckLastFailureReason",
        "route53:getHealthCheckStatus",
        "route53:getHostedZone",
        "route53:getHostedZoneCount",
        "route53:getHostedZoneLimit",
        "route53:getQueryLoggingConfig",
        "route53:getReusableDelegationSet",
        "route53:getTrafficPolicy",
        "route53:getTrafficPolicyInstance",
        "route53:getTrafficPolicyInstanceCount",
        "route53:listCidrBlocks",
        "route53:listCidrCollections",
        "route53:listCidrLocations",
        "route53:listGeoLocations",
        "route53:listHealthChecks",
        "route53:listHostedZones",
        "route53:listHostedZonesByName",
        "route53:listHostedZonesByVpc",
        "route53:listQueryLoggingConfigs",
        "route53:listResourceRecordSets",
        "route53:listReusableDelegationSets",
        "route53:listTrafficPolicies",
        "route53:listTrafficPolicyInstances",
        "route53:listTrafficPolicyInstancesByHostedZone",
        "route53:listTrafficPolicyInstancesByPolicy",
        "route53:listTrafficPolicyVersions",
        "route53:listVPCAssociationAuthorizations",
        "route53domains:checkDomainAvailability",
        "route53domains:getContactReachabilityStatus",
        "route53domains:getDomainDetail",
        "route53domains:getOperationDetail",
        "route53domains:listDomains",
        "route53domains:listOperations",
        "route53domains:listPrices",
        "route53domains:listTagsForDomain",
        "route53domains:viewBilling",
        "route53profiles:getProfile",
        "route53profiles:getProfileAssociation",
```

```
        "route53profiles:getProfileResourceAssociation",
        "route53profiles:listProfileAssociations",
        "route53profiles:listProfileResourceAssociations",
        "route53profiles:listProfiles",
        "route53profiles:listTagsForResource",
        "route53resolver:getFirewallConfig",
        "route53resolver:getFirewallDomainList",
        "route53resolver:getFirewallRuleGroup",
        "route53resolver:getFirewallRuleGroupAssociation",
        "route53resolver:getFirewallRuleGroupPolicy",
        "route53resolver:getOutpostResolver",
        "route53resolver:getResolverDnssecConfig",
        "route53resolver:getResolverQueryLogConfig",
        "route53resolver:getResolverQueryLogConfigAssociation",
        "route53resolver:getResolverQueryLogConfigPolicy",
        "route53resolver:getResolverRule",
        "route53resolver:getResolverRuleAssociation",
        "route53resolver:getResolverRulePolicy",
        "route53resolver:listFirewallConfigs",
        "route53resolver:listFirewallDomainLists",
        "route53resolver:listFirewallDomains",
        "route53resolver:listFirewallRuleGroupAssociations",
        "route53resolver:listFirewallRuleGroups",
        "route53resolver:listFirewallRules",
        "route53resolver:listOutpostResolvers",
        "route53resolver:listResolverConfigs",
        "route53resolver:listResolverDnssecConfigs",
        "route53resolver:listResolverEndpointIpAddresses",
        "route53resolver:listResolverEndpoints",
        "route53resolver:listResolverQueryLogConfigAssociations",
        "route53resolver:listResolverQueryLogConfigs",
        "route53resolver:listResolverRuleAssociations",
        "route53resolver:listResolverRules",
        "route53resolver:listTagsForResource",
        "rum:batchGetRumMetricDefinitions",
        "rum:getAppMonitor",
        "rum:listAppMonitors",
        "rum:listRumMetricsDestinations",
        "s3-outposts:listEndpoints",
        "s3-outposts:listOutpostsWithS3",
        "s3-outposts:listRegionalBuckets",
        "s3-outposts:listSharedEndpoints",
        "s3:describeJob",
        "s3:describeMultiRegionAccessPointOperation",
```

```
        "s3:getAccelerateConfiguration",
        "s3:getAccessGrant",
        "s3:getAccessGrantsInstance",
        "s3:getAccessGrantsInstanceResourcePolicy",
        "s3:getAccessGrantsLocation",
        "s3:getAccessPoint",
        "s3:getAccessPointConfigurationForObjectLambda",
        "s3:getAccessPointForObjectLambda",
        "s3:getAccessPointPolicy",
        "s3:getAccessPointPolicyForObjectLambda",
        "s3:getAccessPointPolicyStatus",
        "s3:getAccessPointPolicyStatusForObjectLambda",
        "s3:getAccountPublicAccessBlock",
        "s3:getAnalyticsConfiguration",
        "s3:getBucketAcl",
        "s3:getBucketCORS",
        "s3:getBucketLocation",
        "s3:getBucketLogging",
        "s3:getBucketNotification",
        "s3:getBucketObjectLockConfiguration",
        "s3:getBucketOwnershipControls",
        "s3:getBucketPolicy",
        "s3:getBucketPolicyStatus",
        "s3:getBucketPublicAccessBlock",
        "s3:getBucketRequestPayment",
        "s3:getBucketVersioning",
        "s3:getBucketWebsite",
        "s3:getEncryptionConfiguration",
        "s3:getIntelligentTieringConfiguration",
        "s3:getInventoryConfiguration",
        "s3:getLifecycleConfiguration",
        "s3:getMetricsConfiguration",
        "s3:getMultiRegionAccessPoint",
        "s3:getMultiRegionAccessPointPolicy",
        "s3:getMultiRegionAccessPointPolicyStatus",
        "s3:getMultiRegionAccessPointRoutes",
        "s3:getObjectAcl",
        "s3:getObjectLegalHold",
        "s3:getObjectRetention",
        "s3:getReplicationConfiguration",
        "s3:getStorageLensConfiguration",
        "s3:listAccessGrants",
        "s3:listAccessGrantsInstances",
        "s3:listAccessGrantsLocations",
```

```
        "s3:listAccessPoints",
        "s3:listAccessPointsForObjectLambda",
        "s3:listAllMyBuckets",
        "s3:listBucket",
        "s3:listBucketMultipartUploads",
        "s3:listBucketVersions",
        "s3:listJobs",
        "s3:listMultipartUploadParts",
        "s3:listMultiRegionAccessPoints",
        "s3:listStorageLensConfigurations",
        "s3express:getBucketPolicy",
        "s3express:listAllMyDirectoryBuckets",
        "s3tables:getNamespace",
        "s3tables:getTable",
        "s3tables:getTableBucket",
        "s3tables:getTableBucketEncryption",
        "s3tables:getTableBucketMaintenanceConfiguration",
        "s3tables:getTableBucketPolicy",
        "s3tables:getTableEncryption",
        "s3tables:getTableMaintenanceConfiguration",
        "s3tables:getTableMaintenanceJobStatus",
        "s3tables:getTableMetadataLocation",
        "s3tables:getTablePolicy",
        "s3tables:listNamespaces",
        "s3tables:listTableBuckets",
        "s3tables:listTables",
        "s3vectors:getIndex",
        "s3vectors:getVectorBucket",
        "s3vectors:getVectorBucketPolicy",
        "s3vectors:listIndexes",
        "s3vectors:listVectorBuckets",
        "sagemaker:describeAction",
        "sagemaker:describeAlgorithm",
        "sagemaker:describeApp",
        "sagemaker:describeAppImageConfig",
        "sagemaker:describeArtifact",
        "sagemaker:describeAutoMLJob",
        "sagemaker:describeCluster",
        "sagemaker:describeClusterNode",
        "sagemaker:describeCodeRepository",
        "sagemaker:describeCompilationJob",
        "sagemaker:describeContext",
        "sagemaker:describeDataQualityJobDefinition",
        "sagemaker:describeDevice",
```

```
        "sagemaker:describeDeviceFleet",
        "sagemaker:describeDomain",
        "sagemaker:describeEdgeDeploymentPlan",
        "sagemaker:describeEdgePackagingJob",
        "sagemaker:describeEndpoint",
        "sagemaker:describeEndpointConfig",
        "sagemaker:describeExperiment",
        "sagemaker:describeFeatureGroup",
        "sagemaker:describeFeatureMetadata",
        "sagemaker:describeFlowDefinition",
        "sagemaker:describeHub",
        "sagemaker:describeHubContent",
        "sagemaker:describeHumanTaskUi",
        "sagemaker:describeHyperParameterTuningJob",
        "sagemaker:describeImage",
        "sagemaker:describeImageVersion",
        "sagemaker:describeInferenceComponent",
        "sagemaker:describeInferenceExperiment",
        "sagemaker:describeInferenceRecommendationsJob",
        "sagemaker:describeLabelingJob",
        "sagemaker:describeMlflowTrackingServer",
        "sagemaker:describeModel",
        "sagemaker:describeModelBiasJobDefinition",
        "sagemaker:describeModelCard",
        "sagemaker:describeModelCardExportJob",
        "sagemaker:describeModelExplainabilityJobDefinition",
        "sagemaker:describeModelPackage",
        "sagemaker:describeModelPackageGroup",
        "sagemaker:describeModelQualityJobDefinition",
        "sagemaker:describeMonitoringSchedule",
        "sagemaker:describeNotebookInstance",
        "sagemaker:describeNotebookInstanceLifecycleConfig",
        "sagemaker:describePipeline",
        "sagemaker:describePipelineDefinitionForExecution",
        "sagemaker:describePipelineExecution",
        "sagemaker:describePartnerApp",
        "sagemaker:describeProcessingJob",
        "sagemaker:describeProject",
        "sagemaker:describeSpace",
        "sagemaker:describeStudioLifecycleConfig",
        "sagemaker:describeSubscribedWorkteam",
        "sagemaker:describeTrainingJob",
        "sagemaker:describeTransformJob",
        "sagemaker:describeTrial",
```

```
        "sagemaker:describeTrialComponent",
        "sagemaker:describeUserProfile",
        "sagemaker:describeWorkforce",
        "sagemaker:describeWorkteam",
        "sagemaker:getDeviceFleetReport",
        "sagemaker:getModelPackageGroupPolicy",
        "sagemaker:getSagemakerServicecatalogPortfolioStatus",
        "sagemaker:listActions",
        "sagemaker:listAlgorithms",
        "sagemaker:listAliases",
        "sagemaker:listAppImageConfigs",
        "sagemaker:listApps",
        "sagemaker:listArtifacts",
        "sagemaker:listAssociations",
        "sagemaker:listAutoMLJobs",
        "sagemaker:listCandidatesForAutoMLJob",
        "sagemaker:listClusterNodes",
        "sagemaker:listClusters",
        "sagemaker:listCodeRepositories",
        "sagemaker:listCompilationJobs",
        "sagemaker:listContexts",
        "sagemaker:listDataQualityJobDefinitions",
        "sagemaker:listDeviceFleets",
        "sagemaker:listDevices",
        "sagemaker:listDomains",
        "sagemaker:listEdgeDeploymentPlans",
        "sagemaker:listEdgePackagingJobs",
        "sagemaker:listEndpointConfigs",
        "sagemaker:listEndpoints",
        "sagemaker:listExperiments",
        "sagemaker:listFeatureGroups",
        "sagemaker:listFlowDefinitions",
        "sagemaker:listHubContents",
        "sagemaker:listHubContentVersions",
        "sagemaker:listHubs",
        "sagemaker:listHumanTaskUis",
        "sagemaker:listHyperParameterTuningJobs",
        "sagemaker:listImages",
        "sagemaker:listImageVersions",
        "sagemaker:listInferenceComponents",
        "sagemaker:listInferenceExperiments",
        "sagemaker:listInferenceRecommendationsJobs",
        "sagemaker:listInferenceRecommendationsJobSteps",
        "sagemaker:listLabelingJobs",
```

```
        "sagemaker:listLabelingJobsForWorkteam",
        "sagemaker:listLineageGroups",
        "sagemaker:listMlflowTrackingServers",
        "sagemaker:listModelBiasJobDefinitions",
        "sagemaker:listModelCardExportJobs",
        "sagemaker:listModelCards",
        "sagemaker:listModelCardVersions",
        "sagemaker:listModelExplainabilityJobDefinitions",
        "sagemaker:listModelMetadata",
        "sagemaker:listModelPackageGroups",
        "sagemaker:listModelPackages",
        "sagemaker:listModelQualityJobDefinitions",
        "sagemaker:listModels",
        "sagemaker:listMonitoringAlertHistory",
        "sagemaker:listMonitoringAlerts",
        "sagemaker:listMonitoringExecutions",
        "sagemaker:listMonitoringSchedules",
        "sagemaker:listNotebookInstanceLifecycleConfigs",
        "sagemaker:listNotebookInstances",
        "sagemaker:listPartnerApps",
        "sagemaker:listPipelineExecutions",
        "sagemaker:listPipelineExecutionSteps",
        "sagemaker:listPipelineParametersForExecution",
        "sagemaker:listPipelines",
        "sagemaker:listProcessingJobs",
        "sagemaker:listProjects",
        "sagemaker:listSpaces",
        "sagemaker:listStageDevices",
        "sagemaker:listStudioLifecycleConfigs",
        "sagemaker:listSubscribedWorkteams",
        "sagemaker:listTags",
        "sagemaker:listTrainingJobs",
        "sagemaker:listTrainingJobsForHyperParameterTuningJob",
        "sagemaker:listTransformJobs",
        "sagemaker:listTrialComponents",
        "sagemaker:listTrials",
        "sagemaker:listUserProfiles",
        "sagemaker:listWorkforces",
        "sagemaker:listWorkteams",
        "savingsplans:describeSavingsPlans",
        "scheduler:getSchedule",
        "scheduler:getScheduleGroup",
        "scheduler:listScheduleGroups",
        "scheduler:listSchedules",
```

```
        "schemas:describeCodeBinding",
        "schemas:describeDiscoverer",
        "schemas:describeRegistry",
        "schemas:describeSchema",
        "schemas:getCodeBindingSource",
        "schemas:getDiscoveredSchema",
        "schemas:getResourcePolicy",
        "schemas:listDiscoverers",
        "schemas:listRegistries",
        "schemas:listSchemas",
        "schemas:listSchemaVersions",
        "sdb:domainMetadata",
        "sdb:listDomains",
        "secretsmanager:describeSecret",
        "secretsmanager:getResourcePolicy",
        "secretsmanager:listSecrets",
        "secretsmanager:listSecretVersionIds",
        "securityhub:batchGetAutomationRules",
        "securityhub:batchGetConfigurationPolicyAssociations",
        "securityhub:describeOrganizationConfiguration",
        "securityhub:getConfigurationPolicy",
        "securityhub:getConfigurationPolicyAssociation",
        "securityhub:getEnabledStandards",
        "securityhub:getFindingAggregator",
        "securityhub:getFindingHistory",
        "securityhub:getFindings",
        "securityhub:getInsightResults",
        "securityhub:getInsights",
        "securityhub:getMasterAccount",
        "securityhub:getMembers",
        "securityhub:listAutomationRules",
        "securityhub:listConfigurationPolicies",
        "securityhub:listConfigurationPolicyAssociations",
        "securityhub:listEnabledProductsForImport",
        "securityhub:listFindingAggregators",
        "securityhub:listInvitations",
        "securityhub:listMembers",
        "securitylake:getDataLakeExceptionSubscription",
        "securitylake:getDataLakeOrganizationConfiguration",
        "securitylake:getDataLakeSources",
        "securitylake:getSubscriber",
        "securitylake:listDataLakeExceptions",
        "securitylake:listDataLakes",
        "securitylake:listLogSources",
```

```
        "securitylake:listSubscribers",
        "serverlessrepo:getApplication",
        "serverlessrepo:getApplicationPolicy",
        "serverlessrepo:getCloudFormationTemplate",
        "serverlessrepo:listApplicationDependencies",
        "serverlessrepo:listApplications",
        "serverlessrepo:listApplicationVersions",
        "servicecatalog:describeConstraint",
        "servicecatalog:describePortfolio",
        "servicecatalog:describeProduct",
        "servicecatalog:describeProductAsAdmin",
        "servicecatalog:describeProductView",
        "servicecatalog:describeProvisioningArtifact",
        "servicecatalog:describeProvisioningParameters",
        "servicecatalog:describeRecord",
        "servicecatalog:listAcceptedPortfolioShares",
        "servicecatalog:listConstraintsForPortfolio",
        "servicecatalog:listLaunchPaths",
        "servicecatalog:listPortfolioAccess",
        "servicecatalog:listPortfolios",
        "servicecatalog:listPortfoliosForProduct",
        "servicecatalog:listPrincipalsForPortfolio",
        "servicecatalog:listProvisioningArtifacts",
        "servicecatalog:listRecordHistory",
        "servicecatalog:scanProvisionedProducts",
        "servicecatalog:searchProducts",
        "servicequotas:getAssociationForServiceQuotaTemplate",
        "servicequotas:getAWSDefaultServiceQuota",
        "servicequotas:getRequestedServiceQuotaChange",
        "servicequotas:getServiceQuota",
        "servicequotas:getServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:listAWSDefaultServiceQuotas",
        "servicequotas:listRequestedServiceQuotaChangeHistory",
        "servicequotas:listRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:listServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:listServiceQuotas",
        "servicequotas:listServices",
        "ses:batchGetMetricData",
        "ses:describeActiveReceiptRuleSet",
        "ses:describeConfigurationSet",
        "ses:describeReceiptRule",
        "ses:describeReceiptRuleSet",
        "ses:getAccount",
        "ses:getAccountSendingEnabled",
```

```
        "ses:getAddonInstance",
        "ses:getAddonSubscription",
        "ses:getArchive",
        "ses:getArchiveExport",
        "ses:getArchiveSearch",
        "ses:getBlacklistReports",
        "ses:getConfigurationSet",
        "ses:getConfigurationSetEventDestinations",
        "ses:getContactList",
        "ses:getDedicatedIp",
        "ses:getDedicatedIpPool",
        "ses:getDedicatedIps",
        "ses:getDeliverabilityDashboardOptions",
        "ses:getDeliverabilityTestReport",
        "ses:getDomainDeliverabilityCampaign",
        "ses:getDomainStatisticsReport",
        "ses:getEmailIdentity",
        "ses:getIdentityDkimAttributes",
        "ses:getIdentityMailFromDomainAttributes",
        "ses:getIdentityNotificationAttributes",
        "ses:getIdentityPolicies",
        "ses:getIdentityVerificationAttributes",
        "ses:getImportJob",
        "ses:getIngressPoint",
        "ses:getMessageInsights",
        "ses:getRelay",
        "ses:getRuleSet",
        "ses:getTrafficPolicy",
        "ses:getSendQuota",
        "ses:getSendStatistics",
        "ses:listConfigurationSets",
        "ses:listAddonInstances",
        "ses:listAddonSubscriptions",
        "ses:listArchiveExports",
        "ses:listArchives",
        "ses:listArchiveSearches",
        "ses:listContactLists",
        "ses:listContacts",
        "ses:listCustomVerificationEmailTemplates",
        "ses:listDedicatedIpPools",
        "ses:listDeliverabilityTestReports",
        "ses:listDomainDeliverabilityCampaigns",
        "ses:listEmailIdentities",
        "ses:listEmailTemplates",
```

```
        "ses:listIdentities",
        "ses:listIdentityPolicies",
        "ses:listImportJobs",
        "ses:listIngressPoints",
        "ses:listReceiptFilters",
        "ses:listReceiptRuleSets",
        "ses:listRelays",
        "ses:listRuleSets",
        "ses:listRecommendations",
        "ses:listTagsForResource",
        "ses:listTemplates",
        "ses:listTrafficPolicies",
        "ses:listVerifiedEmailAddresses",
        "shield:describeAttack",
        "shield:describeProtection",
        "shield:describeSubscription",
        "shield:listAttacks",
        "shield:listProtections",
        "signer:describeSigningJob",
        "signer:getRevocationStatus",
        "signer:getSigningPlatform",
        "signer:getSigningProfile",
        "signer:listProfilePermissions",
        "signer:listSigningJobs",
        "signer:listSigningPlatforms",
        "signer:listSigningProfiles",
        "sms-voice:getConfigurationSetEventDestinations",
        "sms:getConnectors",
        "sms:getReplicationJobs",
        "sms:getReplicationRuns",
        "sms:getServers",
        "snowball:describeAddress",
        "snowball:describeAddresses",
        "snowball:describeJob",
        "snowball:getSnowballUsage",
        "snowball:listJobs",
        "snowball:listServiceVersions",
        "sns:checkIfPhoneNumberIsOptedOut",
        "sns:getDataProtectionPolicy",
        "sns:getEndpointAttributes",
        "sns:getPlatformApplicationAttributes",
        "sns:getSMSAttributes",
        "sns:getSMSSandboxAccountStatus",
        "sns:getSubscriptionAttributes",
```

```
        "sns:getTopicAttributes",
        "sns:listEndpointsByPlatformApplication",
        "sns:listOriginationNumbers",
        "sns:listPhoneNumbersOptedOut",
        "sns:listPlatformApplications",
        "sns:listSMSSandboxPhoneNumbers",
        "sns:listSubscriptions",
        "sns:listSubscriptionsByTopic",
        "sns:listTopics",
        "sqs:getQueueAttributes",
        "sqs:getQueueUrl",
        "sqs:listDeadLetterSourceQueues",
        "sqs:listMessageMoveTasks",
        "sqs:listQueues",
        "ssm-contacts:describeEngagement",
        "ssm-contacts:describePage",
        "ssm-contacts:getContact",
        "ssm-contacts:getContactChannel",
        "ssm-contacts:getContactPolicy",
        "ssm-contacts:getRotation",
        "ssm-contacts:getRotationOverride",
        "ssm-contacts:listContactChannels",
        "ssm-contacts:listContacts",
        "ssm-contacts:listEngagements",
        "ssm-contacts:listPageReceipts",
        "ssm-contacts:listPageResolutions",
        "ssm-contacts:listPagesByContact",
        "ssm-contacts:listPagesByEngagement",
        "ssm-contacts:listPreviewRotationShifts",
        "ssm-contacts:listRotationOverrides",
        "ssm-contacts:listRotations",
        "ssm-contacts:listRotationShifts",
        "ssm-incidents:batchGetIncidentFindings",
        "ssm-incidents:getIncidentRecord",
        "ssm-incidents:getReplicationSet",
        "ssm-incidents:getResourcePolicies",
        "ssm-incidents:getResponsePlan",
        "ssm-incidents:getTimelineEvent",
        "ssm-incidents:listIncidentFindings",
        "ssm-incidents:listIncidentRecords",
        "ssm-incidents:listRelatedItems",
        "ssm-incidents:listReplicationSets",
        "ssm-incidents:listResponsePlans",
        "ssm-incidents:listTimelineEvents",
```

```
            "ssm-quicksetup:getConfiguration",
            "ssm-quicksetup:getConfigurationManager",
            "ssm-quicksetup:getServiceSettings",
            "ssm-quicksetup:listConfigurationManagers",
            "ssm-quicksetup:listConfigurations",
            "ssm-quicksetup:listQuickSetupTypes",
            "ssm-sap:getApplication",
            "ssm-sap:getComponent",
            "ssm-sap:getDatabase",
            "ssm-sap:getOperation",
            "ssm-sap:getResourcePermission",
            "ssm-sap:listApplications",
            "ssm-sap:listComponents",
            "ssm-sap:listDatabases",
            "ssm-sap:listOperations",
            "ssm:describeActivations",
            "ssm:describeAssociation",
            "ssm:describeAssociationExecutions",
            "ssm:describeAssociationExecutionTargets",
            "ssm:describeAutomationExecutions",
            "ssm:describeAutomationStepExecutions",
            "ssm:describeAvailablePatches",
            "ssm:describeDocument",
            "ssm:describeDocumentPermission",
            "ssm:describeEffectiveInstanceAssociations",
            "ssm:describeEffectivePatchesForPatchBaseline",
            "ssm:describeInstanceAssociationsStatus",
            "ssm:describeInstanceInformation",
            "ssm:describeInstancePatches",
            "ssm:describeInstancePatchStates",
            "ssm:describeInstancePatchStatesForPatchGroup",
            "ssm:describeInstanceProperties",
            "ssm:describeInventoryDeletions",
            "ssm:describeMaintenanceWindowExecutions",
            "ssm:describeMaintenanceWindowExecutionTaskInvocations",
            "ssm:describeMaintenanceWindowExecutionTasks",
            "ssm:describeMaintenanceWindows",
            "ssm:describeMaintenanceWindowSchedule",
            "ssm:describeMaintenanceWindowsForTarget",
            "ssm:describeMaintenanceWindowTargets",
            "ssm:describeMaintenanceWindowTasks",
            "ssm:describeOpsItems",
            "ssm:describeParameters",
            "ssm:describePatchBaselines",
```

```
        "ssm:describePatchGroups",
        "ssm:describePatchGroupState",
        "ssm:describePatchProperties",
        "ssm:describeSessions",
        "ssm:getAutomationExecution",
        "ssm:getCalendarState",
        "ssm:getCommandInvocation",
        "ssm:getConnectionStatus",
        "ssm:getDefaultPatchBaseline",
        "ssm:getDeployablePatchSnapshotForInstance",
        "ssm:getInventorySchema",
        "ssm:getMaintenanceWindow",
        "ssm:getMaintenanceWindowExecution",
        "ssm:getMaintenanceWindowExecutionTask",
        "ssm:getMaintenanceWindowExecutionTaskInvocation",
        "ssm:getMaintenanceWindowTask",
        "ssm:getOpsItem",
        "ssm:getOpsMetadata",
        "ssm:getOpsSummary",
        "ssm:getPatchBaseline",
        "ssm:getPatchBaselineForPatchGroup",
        "ssm:getResourcePolicies",
        "ssm:getServiceSetting",
        "ssm:listAssociations",
        "ssm:listAssociationVersions",
        "ssm:listCommandInvocations",
        "ssm:listCommands",
        "ssm:listComplianceItems",
        "ssm:listComplianceSummaries",
        "ssm:listDocumentMetadataHistory",
        "ssm:listDocuments",
        "ssm:listDocumentVersions",
        "ssm:listNodes",
        "ssm:listNodesSummary",
        "ssm:listOpsItemEvents",
        "ssm:listOpsItemRelatedItems",
        "ssm:listOpsMetadata",
        "ssm:listResourceComplianceSummaries",
        "ssm:listResourceDataSync",
        "ssm:listTagsForResource",
        "sso:describeApplication",
        "sso:describeApplicationAssignment",
        "sso:describeApplicationProvider",
        "sso:describeAccountAssignmentCreationStatus",
```

```
        "sso:describeAccountAssignmentDeletionStatus",
        "sso:describeInstance",
        "sso:describeInstanceAccessControlAttributeConfiguration",
        "sso:describePermissionSet",
        "sso:describePermissionSetProvisioningStatus",
        "sso:describeTrustedTokenIssuer",
        "sso:getApplicationAccessScope",
        "sso:getApplicationAssignmentConfiguration",
        "sso:getApplicationAuthenticationMethod",
        "sso:getApplicationGrant",
        "sso:getApplicationInstance",
        "sso:getApplicationTemplate",
        "sso:getInlinePolicyForPermissionSet",
        "sso:getManagedApplicationInstance",
        "sso:getPermissionsBoundaryForPermissionSet",
        "sso:getSharedSsoConfiguration",
        "sso:listApplicationAccessScopes",
        "sso:listApplicationAssignments",
        "sso:listApplicationAuthenticationMethods",
        "sso:listApplicationGrants",
        "sso:listApplicationInstances",
        "sso:listApplicationProviders",
        "sso:listApplications",
        "sso:listApplicationTemplates",
        "sso:listAccountAssignmentCreationStatus",
        "sso:listAccountAssignmentDeletionStatus",
        "sso:listAccountAssignments",
        "sso:listAccountAssignmentsForPrincipal",
        "sso:listAccountsForProvisionedPermissionSet",
        "sso:listApplicationAssignmentsForPrincipal",
        "sso:listCustomerManagedPolicyReferencesInPermissionSet",
        "sso:listDirectoryAssociations",
        "sso:listInstances",
        "sso:listManagedPoliciesInPermissionSet",
        "sso:listPermissionSetProvisioningStatus",
        "sso:listPermissionSets",
        "sso:listPermissionSetsProvisionedToAccount",
        "sso:listProfileAssociations",
        "sso:listTrustedTokenIssuers",
        "states:describeActivity",
        "states:describeExecution",
        "states:describeMapRun",
        "states:describeStateMachine",
        "states:describeStateMachineAlias",
```

```
        "states:describeStateMachineForExecution",
        "states:getExecutionHistory",
        "states:listActivities",
        "states:listExecutions",
        "states:listMapRuns",
        "states:listStateMachineAliases",
        "states:listStateMachines",
        "states:listStateMachineVersions",
        "storagegateway:describeBandwidthRateLimit",
        "storagegateway:describeCache",
        "storagegateway:describeCachediSCSIVolumes",
        "storagegateway:describeFileSystemAssociations",
        "storagegateway:describeGatewayInformation",
        "storagegateway:describeMaintenanceStartTime",
        "storagegateway:describeNFSFileShares",
        "storagegateway:describeSMBFileShares",
        "storagegateway:describeSMBSettings",
        "storagegateway:describeSnapshotSchedule",
        "storagegateway:describeStorediSCSIVolumes",
        "storagegateway:describeTapeArchives",
        "storagegateway:describeTapeRecoveryPoints",
        "storagegateway:describeTapes",
        "storagegateway:describeUploadBuffer",
        "storagegateway:describeVTLDevices",
        "storagegateway:describeWorkingStorage",
        "storagegateway:listAutomaticTapeCreationPolicies",
        "storagegateway:listFileShares",
        "storagegateway:listFileSystemAssociations",
        "storagegateway:listGateways",
        "storagegateway:listLocalDisks",
        "storagegateway:listTagsForResource",
        "storagegateway:listTapes",
        "storagegateway:listVolumeInitiators",
        "storagegateway:listVolumeRecoveryPoints",
        "storagegateway:listVolumes",
        "sts:getCallerIdentity",
        "swf:countClosedWorkflowExecutions",
        "swf:countOpenWorkflowExecutions",
        "swf:countPendingActivityTasks",
        "swf:countPendingDecisionTasks",
        "swf:describeActivityType",
        "swf:describeDomain",
        "swf:describeWorkflowExecution",
        "swf:describeWorkflowType",
```

```
        "swf:getWorkflowExecutionHistory",
        "swf:listActivityTypes",
        "swf:listClosedWorkflowExecutions",
        "swf:listDomains",
        "swf:listOpenWorkflowExecutions",
        "swf:listWorkflowTypes",
        "synthetics:describeCanaries",
        "synthetics:describeCanariesLastRun",
        "synthetics:describeRuntimeVersions",
        "synthetics:getCanary",
        "synthetics:getCanaryRuns",
        "synthetics:getGroup",
        "synthetics:listAssociatedGroups",
        "synthetics:listGroupResources",
        "synthetics:listGroups",
        "thinclient:getDevice",
        "thinclient:getEnvironment",
        "thinclient:getSoftwareSet",
        "thinclient:listDevices",
        "thinclient:listEnvironments",
        "thinclient:listSoftwareSets",
        "timestream:describeAccountSettings",
        "timestream:describeBatchLoadTask",
        "timestream:describeDatabase",
        "timestream:describeEndpoints",
        "timestream:describeScheduledQuery",
        "timestream:describeTable",
        "timestream:listBatchLoadTasks",
        "timestream:listDatabases",
        "timestream:listScheduledQueries",
        "timestream:listTables",
        "tiros:createQuery",
        "tiros:getQueryAnswer",
        "tiros:getQueryExplanation",
        "tnb:getSolFunctionInstance",
        "tnb:getSolFunctionPackage",
        "tnb:getSolNetworkInstance",
        "tnb:getSolNetworkOperation",
        "tnb:getSolNetworkPackage",
        "tnb:listSolFunctionInstances",
        "tnb:listSolFunctionPackages",
        "tnb:listSolNetworkInstances",
        "tnb:listSolNetworkOperations",
        "tnb:listSolNetworkPackages",
```

```
        "transcribe:describeLanguageModel",
        "transcribe:getCallAnalyticsCategory",
        "transcribe:getCallAnalyticsJob",
        "transcribe:getMedicalTranscriptionJob",
        "transcribe:getMedicalVocabulary",
        "transcribe:getTranscriptionJob",
        "transcribe:getVocabulary",
        "transcribe:getVocabularyFilter",
        "transcribe:listCallAnalyticsCategories",
        "transcribe:listCallAnalyticsJobs",
        "transcribe:listLanguageModels",
        "transcribe:listMedicalTranscriptionJobs",
        "transcribe:listMedicalVocabularies",
        "transcribe:listTranscriptionJobs",
        "transcribe:listVocabularies",
        "transcribe:listVocabularyFilters",
        "transfer:describeAccess",
        "transfer:describeAgreement",
        "transfer:describeConnector",
        "transfer:describeExecution",
        "transfer:describeProfile",
        "transfer:describeServer",
        "transfer:describeUser",
        "transfer:describeWebApp",
        "transfer:describeWebAppCustomization",
        "transfer:describeWorkflow",
        "transfer:listAccesses",
        "transfer:listAgreements",
        "transfer:listConnectors",
        "transfer:listExecutions",
        "transfer:listHostKeys",
        "transfer:listProfiles",
        "transfer:listServers",
        "transfer:listTagsForResource",
        "transfer:listUsers",
        "transfer:listWebApps",
        "transfer:listWorkflows",
        "transfer:sendWorkflowStepState",
        "trustedadvisor:getOrganizationRecommendation",
        "trustedadvisor:getRecommendation",
        "trustedadvisor:listChecks",
        "trustedadvisor:listOrganizationRecommendationAccounts",
        "trustedadvisor:listOrganizationRecommendationResources",
        "trustedadvisor:listOrganizationRecommendations",
```

```
        "trustedadvisor:listRecommendationResources",
        "trustedadvisor:listRecommendations",
        "verifiedpermissions:getIdentitySource",
        "verifiedpermissions:getPolicy",
        "verifiedpermissions:getPolicyStore",
        "verifiedpermissions:getPolicyTemplate",
        "verifiedpermissions:getSchema",
        "verifiedpermissions:listIdentitySources",
        "verifiedpermissions:listPolicies",
        "verifiedpermissions:listPolicyStores",
        "verifiedpermissions:listPolicyTemplates",
        "vpc-lattice:getAccessLogSubscription",
        "vpc-lattice:getAuthPolicy",
        "vpc-lattice:getListener",
        "vpc-lattice:getResourceConfiguration",
        "vpc-lattice:getResourceGateway",
        "vpc-lattice:getResourcePolicy",
        "vpc-lattice:getRule",
        "vpc-lattice:getService",
        "vpc-lattice:getServiceNetwork",
        "vpc-lattice:getServiceNetworkResourceAssociation",
        "vpc-lattice:getServiceNetworkServiceAssociation",
        "vpc-lattice:getServiceNetworkVpcAssociation",
        "vpc-lattice:getTargetGroup",
        "vpc-lattice:listAccessLogSubscriptions",
        "vpc-lattice:listListeners",
        "vpc-lattice:listResourceConfigurations",
        "vpc-lattice:listResourceGateways",
        "vpc-lattice:listRules",
        "vpc-lattice:listServiceNetworks",
        "vpc-lattice:listServiceNetworkResourceAssociations",
        "vpc-lattice:listServiceNetworkServiceAssociations",
        "vpc-lattice:listServiceNetworkVpcAssociations",
        "vpc-lattice:listServices",
        "vpc-lattice:listTargetGroups",
        "vpc-lattice:listTargets",
        "waf-regional:getByteMatchSet",
        "waf-regional:getChangeTokenStatus",
        "waf-regional:getGeoMatchSet",
        "waf-regional:getIPSet",
        "waf-regional:getLoggingConfiguration",
        "waf-regional:getRateBasedRule",
        "waf-regional:getRegexMatchSet",
        "waf-regional:getRegexPatternSet",
```

```
        "waf-regional:getRule",
        "waf-regional:getRuleGroup",
        "waf-regional:getSqlInjectionMatchSet",
        "waf-regional:getWebACL",
        "waf-regional:getWebACLForResource",
        "waf-regional:listActivatedRulesInRuleGroup",
        "waf-regional:listByteMatchSets",
        "waf-regional:listGeoMatchSets",
        "waf-regional:listIPSets",
        "waf-regional:listLoggingConfigurations",
        "waf-regional:listRateBasedRules",
        "waf-regional:listRegexMatchSets",
        "waf-regional:listRegexPatternSets",
        "waf-regional:listResourcesForWebACL",
        "waf-regional:listRuleGroups",
        "waf-regional:listRules",
        "waf-regional:listSqlInjectionMatchSets",
        "waf-regional:listWebACLs",
        "waf:getByteMatchSet",
        "waf:getChangeTokenStatus",
        "waf:getGeoMatchSet",
        "waf:getIPSet",
        "waf:getLoggingConfiguration",
        "waf:getRateBasedRule",
        "waf:getRegexMatchSet",
        "waf:getRegexPatternSet",
        "waf:getRule",
        "waf:getRuleGroup",
        "waf:getSampledRequests",
        "waf:getSizeConstraintSet",
        "waf:getSqlInjectionMatchSet",
        "waf:getWebACL",
        "waf:getXssMatchSet",
        "waf:listActivatedRulesInRuleGroup",
        "waf:listByteMatchSets",
        "waf:listGeoMatchSets",
        "waf:listIPSets",
        "waf:listLoggingConfigurations",
        "waf:listRateBasedRules",
        "waf:listRegexMatchSets",
        "waf:listRegexPatternSets",
        "waf:listRuleGroups",
        "waf:listRules",
        "waf:listSizeConstraintSets",
```

```
        "waf:listSqlInjectionMatchSets",
        "waf:listWebACLs",
        "waf:listXssMatchSets",
        "wafv2:checkCapacity",
        "wafv2:describeManagedRuleGroup",
        "wafv2:getIPSet",
        "wafv2:getLoggingConfiguration",
        "wafv2:getPermissionPolicy",
        "wafv2:getRateBasedStatementManagedKeys",
        "wafv2:getRegexPatternSet",
        "wafv2:getRuleGroup",
        "wafv2:getSampledRequests",
        "wafv2:getWebACL",
        "wafv2:getWebACLForResource",
        "wafv2:listAvailableManagedRuleGroups",
        "wafv2:listIPSets",
        "wafv2:listLoggingConfigurations",
        "wafv2:listRegexPatternSets",
        "wafv2:listResourcesForWebACL",
        "wafv2:listRuleGroups",
        "wafv2:listTagsForResource",
        "wafv2:listWebACLs",
        "workdocs:checkAlias",
        "workdocs:describeAvailableDirectories",
        "workdocs:describeInstances",
        "workmail:describeGroup",
        "workmail:describeOrganization",
        "workmail:describeResource",
        "workmail:describeUser",
        "workmail:listAliases",
        "workmail:listGroupMembers",
        "workmail:listGroups",
        "workmail:listMailboxPermissions",
        "workmail:listOrganizations",
        "workmail:listResourceDelegates",
        "workmail:listResources",
        "workmail:listUsers",
        "workspaces-web:getBrowserSettings",
        "workspaces-web:getIdentityProvider",
        "workspaces-web:getNetworkSettings",
        "workspaces-web:getPortal",
        "workspaces-web:getPortalServiceProviderMetadata",
        "workspaces-web:getTrustStoreCertificate",
        "workspaces-web:getUserSettings",
```

```
        "workspaces-web:listBrowserSettings",
        "workspaces-web:listIdentityProviders",
        "workspaces-web:listNetworkSettings",
        "workspaces-web:listPortals",
        "workspaces-web:listTagsForResource",
        "workspaces-web:listTrustStoreCertificates",
        "workspaces-web:listTrustStores",
        "workspaces-web:listUserSettings",
        "workspaces:describeAccount",
        "workspaces:describeAccountModifications",
        "workspaces:describeApplicationAssociations",
        "workspaces:describeIpGroups",
        "workspaces:describeTags",
        "workspaces:describeWorkspaceAssociations",
        "workspaces:describeWorkspaceBundles",
        "workspaces:describeWorkspaceDirectories",
        "workspaces:describeWorkspaceImages",
        "workspaces:describeWorkspaces",
        "workspaces:describeWorkspaceSnapshots",
        "workspaces:describeWorkspacesConnectionStatus",
        "workspaces:describeWorkspacesPools",
        "workspaces:describeWorkspacesPoolSessions",
        "xray:getEncryptionConfig",
        "xray:getGroup",
        "xray:getGroups",
        "xray:getInsightImpactGraph",
        "xray:getSamplingRules",
        "xray:getSamplingStatisticSummaries",
        "xray:getSamplingTargets",
        "xray:getServiceGraph",
        "xray:getTimeSeriesServiceStatistics",
        "xray:getTraceGraph",
        "xray:listResourcePolicies"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerAccountDiscoveryServicePolicy

Beschreibung: Erteilt AWS Systems Manager (SSM) die Erlaubnis, AWS-Konto Informationen zu ermitteln.

`AWSSystemsManagerAccountDiscoveryServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2019, 17:21 Uhr UTC
- Zeit bearbeitet: 17. Oktober 2022, 20:25 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerAccountDiscoveryServicePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListDelegatedServicesForAccount",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerChangeManagementServicePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die vom AWS Systems Manager Change Management Framework verwaltet oder verwendet werden.

`AWSSystemsManagerChangeManagementServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Dezember 2020, 22:21 Uhr UTC
- Bearbeitete Zeit: 23. Oktober 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerChangeManagementServicePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:DeleteAssociation",
        "ssm:CreateOpsItem",
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "ssm:GetAutomationExecution",
```

```
        "ssm:GetCalendarState",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ssm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerEnableConfigRecordingExecutionPolicy

Beschreibung: Stellt Berechtigungen für AWS Systems Manager Quick Setup bereit, um die Aufzeichnung der AWS Konfigurationskonfiguration zu aktivieren und zu konfigurieren.

`AWSSystemsManagerEnableConfigRecordingExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerEnableConfigRecordingExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:40 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:40 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableConfigRecordingExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "S3BucketCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPublicAccessBlock",
        "s3:ListBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-quick-setup-config-recording-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SNSTopicsListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DefaultSNSTopicCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:ConfigRecording-Default-Topic"
    },
    {
      "Sid" : "ConfigureAndStartConfigurationRecorderPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeDeliveryChannels",
        "config:PutConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:StartConfigurationRecorder"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GetAndPassConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig",
        "arn:aws:iam::*:role/AWSServiceRoleForConfig"
      ]
    },
    {
      "Sid" : "CreateConfigSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "config.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerEnableExplorerExecutionPolicy

Beschreibung: Diese Richtlinie gewährt Administratorberechtigungen für die Aktivierung von Explorer, einer Funktion von AWS Systems Manager. Dazu gehören Berechtigungen zum Aktualisieren verwandter Systems Manager-Diensteinstellungen und zum Erstellen einer dienstbezogenen Rolle für Systems Manager.

`AWSSystemsManagerEnableExplorerExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerEnableExplorerExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juni 2024, 09:42 UTC
- Bearbeitete Zeit: 26. Juni 2024, 09:42 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateSystemsManagerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ReadOnlyPermissionsForEnablingExplorer",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "config:DescribeConfigurationRecorders",
        "compute-optimizer:GetEnrollmentStatus",
        "support:DescribeTrustedAdvisorChecks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMExplorerServiceSettingsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/ssm-patchmanager",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/EC2",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ExplorerOnboarded",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/Association",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ComputeOptimizer",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/ConfigCompliance",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/OpsData-TrustedAdvisor",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/SupportCenterCase"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerForSAPFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Systems Manager for SAP-Service

`AWSSystemsManagerForSAPFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerForSAPFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2022, 02:11 Uhr UTC
- Bearbeitete Zeit: 10. Juli 2024, 21:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsSsmForSapPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    },
    {
      "Sid" : "AwsSsmForSapServiceRoleCreationPermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-sap.amazonaws.com/
AWSServiceRoleForAWSSSMForSAP"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "ssm-sap.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "Ec2StartStopPermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StartInstances",
```

```
        "ec2:StopInstances"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEqualsIgnoreCase" : {
          "ec2:resourceTag/SSMForSAPManaged" : "True"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerForSAPReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den AWS Systems Manager for SAP-Service

`AWSSystemsManagerForSAPReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerForSAPReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. November 2022, 02:11 Uhr UTC
- Zeit bearbeitet: 17. November 2022, 02:11 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerForSAPReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm-sap:get*",
        "ssm-sap:list*"
      ],
      "Resource" : "arn:*:ssm-sap:*:*:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerJustInTimeAccessServicePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die vom AWS Systems Manager verwaltet oder verwendet werden, ein Just-in-Time-Access-Framework.

`AWSSystemsManagerJustInTimeAccessServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. April 2025, 20:07 UTC
- Bearbeitete Zeit: 23. Oktober 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerJustInTimeAccessServicePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowOpsItemReplication",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemReplicationTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "Replica"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAutomationExecutionTagging",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:automation-execution/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
```

```
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOpsItemManagement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:opsitem/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowRetrieveDocument",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : [
            "ManualApprovalPolicy",
            "AutoApprovalPolicy"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDescriptions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DescribeOpsItems",
        "ssm:DescribeSessions",
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowListTagsForManagedInstances",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:managed-instance/*"
      ]
    },
    {
      "Sid" : "AllowListSSMGUIConnections",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:ListConnections"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetUserId"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSODirectoryActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUsers",
        "sso-directory:IsMemberInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOInstanceActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowDescribingEC2Tags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPublishingCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SSM/JustInTimeAccess"
        }
```

```
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerJustInTimeAccessTokenPolicy

Beschreibung: Die verwaltete Richtlinie AWSSystems ManagerJustInTimeAccessTokenPolicy ermöglicht es Systems Manager, Zugriffstoken zu generieren, die für den just-in-time Knotenzugriff verwendet werden.

`AWSSystemsManagerJustInTimeAccessTokenPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerJustInTimeAccessTokenPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. April 2025, 21:07 UTC
- Bearbeitete Zeit: 25. September 2025, 20:04 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "TerminateAndResumeSessionAndOpenDataChannel",
      "Effect" : "Allow",
      "Action" : [
        "ssm:TerminateSession",
        "ssm:ResumeSession",
        "ssmmessages:OpenDataChannel"
      ],
      "Resource" : "arn:aws:ssm:*:*:session/*"
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

Beschreibung: Die verwaltete Richtlinie AWSSystems ManagerJustInTimeAccessTokenSessionPolicy ermöglicht es Systems Manager, Berechtigungen mit

eingeschränktem Geltungsbereich auf eine just-in-time Knotenzugriffssitzung anzuwenden, sobald diese gestartet wurde.

`AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 17. April 2025, 20:52 UTC
- Bearbeitete Zeit: 17. April 2025, 20:52 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeAccessTokenSessionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SsmStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
```

```
        "arn:aws:ssm:*:*:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Sid" : "GuiConnect",
      "Effect" : "Allow",
      "Action" : [
        "ssm-guiconnect:CancelConnection",
        "ssm-guiconnect:GetConnection",
        "ssm-guiconnect:StartConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SessionManagerKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RdpKmsPermission",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm-guiconnect.*.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "RdpStartSession",
      "Effect" : "Allow",
      "Action" : [
        "ssm:StartSession"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetup",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListDirectoryAssociations*",
        "identitystore:DescribeUser",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SsmRdpSsoSetupSendCommand",
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "ssm-guiconnect.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

Beschreibung: Diese Richtlinie ermöglicht es Systems Manager, eine Zugriffsverweigerungsrichtlinie für den just-in-time Knotenzugriff vom delegierten Administratorkonto an Mitgliedskonten weiterzugeben und die Richtlinie auf mehrere Regionen zu replizieren.

`AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. April 2025, 20:52 UTC
- Bearbeitete Zeit: 23. April 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QuickSetupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm-quicksetup:ListConfigurationManagers",
        "ssm-quicksetup:GetConfigurationManager",
        "cloudformation:ListStackSets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupOrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "ssm-quicksetup.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "QuickSetupSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup"
      ]
    },
    {
      "Sid" : "OrganizationsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMDocumentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetDocument",
        "ssm:DescribeDocument",
        "ssm:ListTagsForResource",
        "ssm:PutResourcePolicy",
        "ssm:DeleteResourcePolicy",
        "ssm:GetResourcePolicies"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy"
        }
      }
    },
    {
      "Sid" : "SSMDocumentCreateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateDocument"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
```

```
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SSMDocumentUpdateReplicaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateDocument",
        "ssm:UpdateDocumentDefaultVersion",
        "ssm:UpdateDocumentMetadata",
        "ssm:DeleteDocument",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:document/SSM-JustInTimeAccessDenyAccessOrgPolicy",
      "Condition" : {
        "StringEquals" : {
          "ssm:DocumentType" : "AutoApprovalPolicy",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    },
    {
      "Sid" : "RAMTaggingPermissions",
      "Effect" : "Allow",
      "Action" : "ram:TagResource",
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "SystemsManagerJustInTimeNodeAccessManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RAMModificationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:ResourceShareName" : "SSMJustInTimeNodeAccessManagedResourceShare",
          "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged" : "true"
```

```
        },
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "ssm:Document"
        },
        "ArnLikeIfExists" : {
          "ram:ResourceArn" : "arn:aws:ssm:*:*:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerNotificationsServicePolicy

Beschreibung: Erforderliche Berechtigungen, um Informationen über einen Benutzer für Just-In-Time-Node -Access-Benachrichtigungen zu sammeln.

`AWSSystemsManagerNotificationsServicePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. April 2025, 20:52 UTC
- Bearbeitete Zeit: 17. April 2025, 20:52 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerNotificationsServicePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowIdentityStoreActions",
      "Effect" : "Allow",
      "Action" : [
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroupMemberships",
        "identitystore:DescribeUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowSSOActions",
      "Effect" : "Allow",
      "Action" : [
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:ListDirectoryAssociations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Sid" : "AllowSSODirectoryActions",
      "Effect" : "Allow",
      "Action" : [
        "sso-directory:DescribeUser",
        "sso-directory:ListMembersInGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowIamActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSSystemsManagerOpsDataSyncServiceRolePolicy

Beschreibung: IAM-Rolle für SSM Explorer zur Verwaltung OpsData verwandter Operationen

`AWSSystemsManagerOpsDataSyncServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. April 2021, 20:42 UTC
- Bearbeitete Zeit: 28. Juni 2023, 22:53 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSSystemsManagerOpsDataSyncServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ExplorerSecurityHubOpsItem" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateOpsItem"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:UpdateServiceSetting",
        "ssm:GetServiceSetting"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*",
        "arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "securityhub:GetFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "securityhub:ASFFSyntaxPath/Workflow.Status" : "SUPPRESSED"
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Confidence" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Criticality" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.Text" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Note.UpdatedBy" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/RelatedFindings" : false
        }
```

```
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/Types" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.key" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/UserDefinedFields.value" : false
        }
      }
    },
    {
      "Effect" : "Deny",
      "Action" : "securityhub:BatchUpdateFindings",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "securityhub:ASFFSyntaxPath/VerificationState" : false
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAssetServerPolicy

Beschreibung: Diese Richtlinie gewährt dem AWS Portal Asset Server die erforderlichen Berechtigungen, die für den normalen Betrieb erforderlich sind.

`AWSThinkboxAssetServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxAssetServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:18 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:18 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAssetServerPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalAdminPolicy

Beschreibung: Diese Richtlinie gewährt der Deadline-Software von AWS Thinkbox vollen Zugriff auf mehrere AWS Dienste, die für die AWS Portalverwaltung erforderlich sind. Dies beinhaltet den Zugriff auf die Erstellung beliebiger Tags für verschiedene EC2 Ressourcentypen.

`AWSThinkboxAWSPortalAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxAWSPortalAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:41 UTC
- Zeit bearbeitet: 12. November 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalAdminPolicy`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxAWSPortal1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AllocateAddress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateInternetGateway",
```

```
        "ec2:CreateNatGateway",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAddresses",
        "ec2:DescribeFleets",
        "ec2:DescribeFleetHistory",
        "ec2:DescribeFleetInstances",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNatGateways",
        "ec2:DescribeTags",
        "ec2:DescribeKeyPairs",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeRegions",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:GetConsoleOutput",
        "ec2:ImportKeyPair",
        "ec2:ReleaseAddress",
        "ec2:RequestSpotFleet",
        "ec2:CancelSpotFleetRequests",
        "ec2:DisassociateAddress",
        "ec2:DeleteFleets",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteVpc",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteInternetGateway",
```

```
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DeleteNatGateway",
        "ec2:DetachInternetGateway",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifyFleet",
        "ec2:ModifySpotFleetRequest",
        "ec2:ModifyVpcAttribute"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal2",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal3",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:InstanceProfile" : "arn:aws:iam::*:instance-profile/AWSPortal*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal4",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/aws:cloudformation:logical-id" : "ReverseForwarder"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal5",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : false
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal6",
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ArnLike" : {
          "ec2:PlacementGroup" : "arn:aws:ec2:*:*:placement-group/
*DeadlinePlacementGroup*"
        }
```

```
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal9",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:natgateway/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal10",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal11",
      "Effect" : "Allow",
```

```
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal12",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetPolicy",
        "iam:ListEntitiesForPolicy",
        "iam:ListPolicyVersions"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/AWSPortal*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal13",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal14",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSPortal*",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "ec2.amazonaws.com",
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal15",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "ec2fleet.amazonaws.com",
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal16",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:PutBucketAcl",
        "s3:PutBucketCORS",
        "s3:PutBucketVersioning",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:PutBucketLogging",
        "s3:PutBucketTagging",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
```

```
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectVersion"
      ],
      "Resource" : [
        "arn:aws:s3::*:awsportal*",
        "arn:aws:s3::*:stack*",
        "arn:aws:s3::*:aws-portal-cache*",
        "arn:aws:s3::*:logs-for-aws-portal-cache*",
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal17",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-aws-portal-cache*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal18",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketOwnershipControls"
      ],
      "Resource" : [
        "arn:aws:s3::*:logs-for-stack*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal19",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal20",
      "Effect" : "Allow",
```

```
      "Action" : [
        "dynamodb:Scan"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal21",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResources",
        "cloudformation:DeleteStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:ListStackResources",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/stack*/*",
        "arn:aws:cloudformation:*:*:stack/Deadline*/*"
      ]
    },
    {
      "Sid" : "AWSThinkboxAWSPortal22",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:EstimateTemplateCost",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal23",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "logs:PutRetentionPolicy",
```

```
        "logs:DeleteRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/thinkbox*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal24",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AWSThinkboxAWSPortal25",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal26",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : [
            "rcs-tls-pw*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxAWSPortal27",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalGatewayPolicy

Beschreibung: Diese Richtlinie gewährt dem AWS Portal Gateway-Computer die für den normalen Betrieb erforderlichen Berechtigungen.

`AWSThinkboxAWSPortalGatewayPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxAWSPortalGatewayPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 27. Mai 2020, 19:05 UTC
- Bearbeitete Zeit: 30. Juni 2020, 16:02 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalGatewayPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "dynamodb:Scan",
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "arn:aws:secretsmanager:*:*:secret:rcs-tls-pw-stack*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxAWSPortalWorkerPolicy

Beschreibung: Diese Richtlinie gewährt den Deadline Workers im AWS Portal die erforderlichen Berechtigungen, die für den normalen Betrieb erforderlich sind.

`AWSThinkboxAWSPortalWorkerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxAWSPortalWorkerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:15 UTC
- Zeit bearbeitet: 7. Dezember 2020, 23:27 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxAWSPortalWorkerPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineRole" : "DeadlineRenderNode"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-portal-cache*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::stack*/gateway_certs/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/thinkbox*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:SendMessage",
        "sqs:GetQueueUrl"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWS*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineResourceTrackerAccessPolicy

Beschreibung: Erteilt die für den Betrieb des Deadline Resource Trackers von AWS Thinkbox erforderlichen Berechtigungen. Dies beinhaltet den vollen Zugriff auf einige EC2 Aktionen, einschließlich DeleteFleets und CancelSpotFleetRequests.

`AWSThinkboxDeadlineResourceTrackerAccessPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxDeadlineResourceTrackerAccessPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:25 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:25 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAccessPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListStreams"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:PutItem",
        "dynamodb:Scan",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateTable"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DeleteFleets",
```

```
        "ec2:DescribeFleetInstances",
        "ec2:DescribeFleets",
        "ec2:DescribeInstances",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "events:PutEvents"
      ],
      "Resource" : [
        "arn:aws:events:*:*:event-bus/default"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/DeadlineResourceTracker*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ReceiveMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeStateMessageQueue*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineResourceTrackerAdminPolicy

Beschreibung: Erteilt die erforderlichen Berechtigungen, um den Deadline Resource Tracker von AWS Thinkbox zu erstellen, zu löschen und zu verwalten.

`AWSThinkboxDeadlineResourceTrackerAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxDeadlineResourceTrackerAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:29 UTC
- Zeit bearbeitet: 12. November 2024, 19:29 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineResourceTrackerAdminPolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker1",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
```

```
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker2",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker3",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:TagResource",
        "cloudformation:UntagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker4",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:CreateTable",
        "dynamodb:DeleteTable",
        "dynamodb:DescribeTable",
        "dynamodb:ListTagsOfResource",
```

```
        "dynamodb:TagResource",
        "dynamodb:UntagResource"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeHealth*",
        "arn:aws:dynamodb:*:*:table/DeadlineEC2ComputeNodeInfo*",
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker5",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan"
      ],
      "Resource" : [
        "arn:aws:dynamodb:*:*:table/DeadlineFleetHealth*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker6",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DescribeRule",
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker7",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTracker*"
      ]
```

```
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker8",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker9",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker10",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DeadlineResourceTrackerAccess*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker11",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/dynamodb.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_DynamoDBTable"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "application-autoscaling.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker12",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker13",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateEventSourceMapping",
        "lambda:DeleteEventSourceMapping"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "lambda:FunctionArn" : [
            "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker14",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:RemovePermission"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ],
      "Condition" : {
        "StringLike" : {
          "lambda:Principal" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker15",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:DeleteFunctionConcurrency",
        "lambda:GetFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListTags",
        "lambda:PutFunctionConcurrency",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:DeadlineResourceTracker*"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker16",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
```

```
      ],
      "Resource" : [
        "arn:aws:s3:::*/deadline_aws_resource_tracker-*.zip",
        "arn:aws:s3:::*/DeadlineAWSResourceTrackerTemplate-*.yaml"
      ]
    },
    {
      "Sid" : "AWSThinkboxDeadlineResourceTracker17",
      "Effect" : "Allow",
      "Action" : [
        "sqs:CreateQueue",
        "sqs:DeleteQueue",
        "sqs:GetQueueAttributes",
        "sqs:ListQueueTags",
        "sqs:TagQueue",
        "sqs:UntagQueue"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*",
        "arn:aws:sqs:*:*:DeadlineResourceTracker*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineSpotEventPluginAdminPolicy

Beschreibung: Erteilt die für das Deadline Spot Event Plugin von AWS Thinkbox erforderlichen Berechtigungen. Dazu gehören die Erlaubnis, eine Spot-Flotte anzufordern, zu ändern und zu stornieren, sowie eingeschränkte PassRole Genehmigungen.

`AWSThinkboxDeadlineSpotEventPluginAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxDeadlineSpotEventPluginAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:38 UTC
- Bearbeitete Zeit: 27. Mai 2020, 19:38 UTC
- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginAdminPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CancelSpotFleetRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2spot:fleet-request-id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
```

```
        "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role",
        "arn:aws:iam::*:role/DeadlineSpot*"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSThinkboxDeadlineSpotEventPluginWorkerPolicy

Beschreibung: Erteilen Sie die erforderlichen Berechtigungen für eine EC2 Instanz, auf der die AWS Thinkbox Deadline Spot Event Plugin Worker-Software ausgeführt wird.

`AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSThinkboxDeadlineSpotEventPluginWorkerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Mai 2020, 19:35 UTC
- Bearbeitete Zeit: 7. Dezember 2020, 23:31 UTC

- ARN: `arn:aws:iam::aws:policy/AWSThinkboxDeadlineSpotEventPluginWorkerPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineTrackedAWSResource" : "SpotEventPlugin"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/DeadlineResourceTracker" : "SpotEventPlugin"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueUrl",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:DeadlineAWSComputeNodeState*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Transfer über AWS-Managementkonsole

`AWSTransferConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransferConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Dezember 2020, 19:33 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "ec2:DescribeAddresses",
```

```
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "health:DescribeEventAggregates",
        "iam:GetPolicyVersion",
        "iam:ListPolicies",
        "iam:ListRoles",
        "route53:ListHostedZones",
        "s3:ListAllMyBuckets",
        "transfer:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferFullAccess

Beschreibung: Bietet vollen Zugriff auf den AWS Transfer-Service.

`AWSTransferFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransferFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 14. Dezember 2020, 19:37 UTC
- Bearbeitete Zeit: 14. Dezember 2020, 19:37 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "transfer:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferLoggingAccess

Beschreibung: Ermöglicht AWS Transfer vollen Zugriff, um Protokollstreams und -gruppen zu erstellen und Protokollereignisse in Ihrem Konto zu speichern

`AWSTransferLoggingAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransferLoggingAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2019, 15:32 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2019, 15:32 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransferLoggingAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransferReadOnlyAccess

Beschreibung: Ermöglichen Sie Lesezugriff auf die AWS Transferdienste.

`AWSTransferReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransferReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. August 2020, 17:54 Uhr UTC
- Bearbeitete Zeit: 27. August 2020, 17:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransferReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransformApplicationDeploymentPolicy

Beschreibung: Ermöglicht dem AWS Transform-Dienst, transformierte .NET-Anwendungen bereitzustellen, indem AWS Ressourcen erstellt und verwaltet werden. Diese Richtlinie gewährt Berechtigungen zur Bereitstellung der Infrastruktur, zur Verwaltung von Rechenressourcen und zur Konfiguration von Bereitstellungseinstellungen für verschiedene AWS Dienste.

`AWSTransformApplicationDeploymentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransformApplicationDeploymentPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 28. August 2025, 06:34 UTC
- Bearbeitete Zeit: 21. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationDeploymentPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/AWSTransform*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "AWSTransform",
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInternetGateways"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Deny",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "ForAnyValue:StringNotEquals" : {
          "aws:TagKeys" : [
            "Name",
            "CreatedBy",
            "ApplicationName",
            "TransformationType",
```

```
            "aws:cloudformation:stack-name",
            "aws:cloudformation:logical-id",
            "aws:cloudformation:stack-id"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*::image/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role",
        "arn:aws:iam::*:instance-profile/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      },
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-Builder-Instance-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-App-Instance-Role"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/ami-amazon-linux-latest*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:ModifyInstanceAttribute"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "cloudformation.amazonaws.com"
        }
      },
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWS-RunRemoteScript"
      ]
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:SendCommand"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:PutBucketTagging"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-transform-deployment-bucket-*",
        "arn:aws:s3:::aws-transform-deployment-bucket-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedFor" : "AWSTransform",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws-transform" : "*",
          "kms:ViaService" : "s3.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ebs:id" : "*"
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com",
          "kms:EncryptionContext:aws:ebs:id" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransformApplicationECSDeploymentPolicy

Beschreibung: Ermöglicht AWS Transform die Bereitstellung von Anwendungen für Amazon Elastic Container Service (ECS) mit Fargate. Es gewährt Berechtigungen zur Bereitstellung, Konfiguration und Verwaltung der zugrunde liegenden Infrastruktur, die für die Ausführung von Anwendungen auf ECS erforderlich ist.

`AWSTransformApplicationECSDeploymentPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransformApplicationECSDeploymentPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. September 2025, 22:49 UTC
- Bearbeitete Zeit: 21. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/AWSTransformApplicationECSDeploymentPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudformation:CreateStack",
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateCluster",
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateCluster",
        "ecs:DeleteCluster"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RegisterTaskDefinition",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:RunTask",
      "Resource" : "arn:aws:ecs:*:*:task-definition/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/CreatedBy" : "AWSTransform"
```

```
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:ListTasks",
      "Resource" : "arn:aws:ecs:*:*:container-instance/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:DescribeTasks",
      "Resource" : "arn:aws:ecs:*:*:task/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "ecs:cluster" : "arn:aws:ecs:*:*:cluster/AWSTransform*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "iam:PassedToService" : [
            "ecs-tasks.amazonaws.com",
```

```
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Task-Role",
        "arn:aws:iam::*:role/AWSTransform-Deploy-ECS-Execution-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ecs:CreateService",
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateService",
        "ecs:DeleteService"
      ],
      "Resource" : "arn:aws:ecs:*:*:service/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "ecs:ResourceTag/CreatedBy" : "AWSTransform"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:TagResource",
        "ecs:UntagResource"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/AWSTransform*",
        "arn:aws:ecs:*:*:task-definition/AWSTransform*",
        "arn:aws:ecs:*:*:service/AWSTransform*",
        "arn:aws:ecs:*:*:task/AWSTransform*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
```

```
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:UntagResource",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:GetLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/ecs/AWSTransform*:log-stream:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:TagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/awstransform*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:RequestTag/CreatedBy" : "AWSTransform"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "ResourceName",
            "CreatedBy",
            "TransformationType"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeServices",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ecs.amazonaws.com/
AWSServiceRoleForECS",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "ecs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "ecr.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:ecr:arn" : "*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:GrantConstraintType" : "EncryptionContextSubset"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransformCustomExecuteTransformations

Beschreibung: Ermöglicht den Zugriff auf die Ausführung von Transformationen in AWS Transform custom.

`AWSTransformCustomExecuteTransformations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransformCustomExecuteTransformations` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Dezember 2025, 15:34 UTC
- Bearbeitungszeit: 5. Dezember 2025, 15:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomExecuteTransformations`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomExecuteTransformations",
```

```
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:ExecuteTransformation",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransformCustomFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Transform Custom.

`AWSTransformCustomFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransformCustomFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Dezember 2025, 15:19 Uhr UTC
- Bearbeitete Zeit: 5. Dezember 2025, 15:19 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomAllActions",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTransformCustomManageTransformations

Beschreibung: Ermöglicht die Verwaltung von Transformationsressourcen und die Ausführung von Transformationen in AWS Transform custom.

`AWSTransformCustomManageTransformations`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTransformCustomManageTransformations` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Dezember 2025, 15:49 UTC
- Bearbeitete Zeit: 5. Dezember 2025, 15:49 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTransformCustomManageTransformations`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSTransformCustomManageTransformations",
      "Effect" : "Allow",
      "Action" : [
        "transform-custom:ConverseStream",
        "transform-custom:CreateTransformationPackageUrl",
        "transform-custom:CompleteTransformationPackageUpload",
        "transform-custom:DeleteTransformationPackage",
        "transform-custom:GetTransformationPackageUrl",
        "transform-custom:ListTransformationPackageMetadata",
        "transform-custom:ExecuteTransformation",
```

```
        "transform-custom:ListKnowledgeItems",
        "transform-custom:GetKnowledgeItem",
        "transform-custom:DeleteKnowledgeItem",
        "transform-custom:UpdateKnowledgeItemConfiguration",
        "transform-custom:UpdateKnowledgeItemStatus",
        "transform-custom:GetCampaign",
        "transform-custom:UpdateCampaignRepositoryStatus",
        "transform-custom:UpdateCampaign",
        "transform-custom:ListTagsForResource",
        "transform-custom:TagResource",
        "transform-custom:UntagResource"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorPriorityFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS Trusted Advisor Priority. Diese Richtlinie ermöglicht es dem Benutzer auch, Trusted Advisor als vertrauenswürdigen Dienst bei AWS Organizations hinzuzufügen und delegierte Administratorkonten für Trusted Advisor Priority anzugeben.

`AWSTrustedAdvisorPriorityFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTrustedAdvisorPriorityFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 16:08 UTC
- Bearbeitete Zeit: 16. August 2022, 16:08 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:UpdateRiskStatus",
        "trustedadvisor:DescribeNotificationConfigurations",
        "trustedadvisor:UpdateNotificationConfigurations",
        "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
        "trustedadvisor:SetOrganizationAccess"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:EnableAWSServiceAccess",
        "organizations:DisableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "reporting.trustedadvisor.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource" : "arn:aws:organizations::*:*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorPriorityReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Trusted Advisor Priority. Dies beinhaltet die Berechtigung, die delegierten Administratorkonten einzusehen.

`AWSTrustedAdvisorPriorityReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSTrustedAdvisorPriorityReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. August 2022, 16:35 UTC
- Bearbeitete Zeit: 16. August 2022, 16:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSTrustedAdvisorPriorityReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeAccount*",
        "trustedadvisor:DescribeOrganization",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:DownloadRisk",
        "trustedadvisor:DescribeNotificationConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "reporting.trustedadvisor.amazonaws.com"
          ]
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorReportingServiceRolePolicy

Beschreibung: Servicerichtlinie für Trusted Advisor Multi-Account-Reporting

`AWSTrustedAdvisorReportingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. November 2019, 17:41 Uhr UTC
- Bearbeitete Zeit: 28. Februar 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorReportingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSTrustedAdvisorServiceRolePolicy

Beschreibung: Zugriff auf den AWS Trusted Advisor Service, um Kosten zu senken, die Leistung zu steigern und die Sicherheit Ihrer AWS Umgebung zu verbessern.

`AWSTrustedAdvisorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Februar 2018, 21:24 UTC
- Bearbeitete Zeit: 30. Oktober 2024, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSTrustedAdvisorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "TrustedAdvisorServiceRolePermissions",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:ListAnalyzers",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "cloudformation:DescribeAccountLimits",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks",
        "cloudfront:ListDistributions",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:GetTrail",
        "cloudtrail:ListTrails",
        "cloudtrail:GetEventSelectors",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "dax:DescribeClusters",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeAddresses",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeImages",
        "ec2:DescribeNatGateways",
        "ec2:DescribeVolumes",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:GetManagedPrefixListEntries",
        "ecs:DescribeTaskDefinition",
        "ecs:ListTaskDefinitions",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth",
        "iam:GenerateCredentialReport",
        "iam:GetAccountPasswordPolicy",
        "iam:GetAccountSummary",
        "iam:GetCredentialReport",
        "iam:GetServerCertificate",
        "iam:ListServerCertificates",
        "iam:ListSAMLProviders",
        "kinesis:DescribeLimits",
        "kafka:DescribeClusterV2",
        "kafka:ListClustersV2",
        "kafka:ListNodes",
        "network-firewall:ListFirewalls",
        "network-firewall:DescribeFirewall",
        "outposts:ListAssets",
        "outposts:GetOutpost",
        "outposts:ListOutposts",
        "rds:DescribeAccountAttributes",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSnapshots",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroupOptions",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribeReservedDBInstances",
        "rds:DescribeReservedDBInstancesOfferings",
        "rds:ListTagsForResource",
        "redshift:DescribeClusters",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "route53:GetAccountLimit",
        "route53:GetHealthCheck",
        "route53:GetHostedZone",
        "route53:ListHealthChecks",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
```

```
        "route53resolver:ListResolverEndpoints",
        "route53resolver:ListResolverEndpointIpAddresses",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "ses:GetSendQuota",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSUserAttributeCostAllocationPolicy

Beschreibung: Bietet schreibgeschützten Zugriff auf Benutzerattribute von AWS IAM Identity Center für die Benutzerattribute, für die sich der Kunde entschieden hat.

`AWSUserAttributeCostAllocationPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Dezember 2025, 16:34 UTC
- Bearbeitete Zeit: 15. Dezember 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserAttributeCostAllocationPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/user-attribute-cost-
allocation-data.amazonaws.com/AWSServiceRoleForUserAttributeCostAllocation"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSUserNotificationsServiceLinkedRolePolicy

Beschreibung: Ermöglicht AWS Benutzerbenachrichtigungen, AWS Dienste in Ihrem Namen aufzurufen.

`AWSUserNotificationsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. April 2023, 13:28 UTC
- Bearbeitete Zeit: 02. September 2025, 20:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSUserNotificationsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
```

```
        "events:PutRule",
        "events:PutTargets",
        "events:DeleteRule",
        "events:ListTargetsByRule",
        "events:RemoveTargets"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AWSUserNotificationsManagedRule-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Notifications"
        }
      },
      "Resource" : "*"
    },
    {
      "Sid" : "AllowOrgsActions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAdminDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
```

```
            "notifications.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "OrganizationNotificationConfigurationDistribution",
      "Effect" : "Allow",
      "Action" : [
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteNotificationConfiguration",
        "notifications:CreateEventRule",
        "notifications:UpdateEventRule",
        "notifications:DeleteEventRule"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsAssessorFullAccess

Beschreibung: Bietet vollen Zugriff zum Anzeigen berechtigter Vendor Insights-Ressourcen und zum Verwalten von Vendor Insights-Abonnements

`AWSVendorInsightsAssessorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSVendorInsightsAssessorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:51 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetProfileAccessTerms",
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:CreateAgreementRequest",
        "aws-marketplace:GetAgreementRequest",
        "aws-marketplace:AcceptAgreementRequest",
        "aws-marketplace:CancelAgreementRequest",
        "aws-marketplace:ListAgreementRequests",
        "aws-marketplace:SearchAgreements",
        "aws-marketplace:CancelAgreement"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsAssessorReadOnly

Beschreibung: Bietet Lesezugriff zum Anzeigen berechtigter Ressourcen von Vendor Insights

`AWSVendorInsightsAssessorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSVendorInsightsAssessorReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:55 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsAssessorReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:ListEntitledSecurityProfiles",
        "vendor-insights:GetEntitledSecurityProfileSnapshot",
        "vendor-insights:ListEntitledSecurityProfileSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsVendorFullAccess

Beschreibung: Bietet vollen Zugriff auf die Erstellung und Verwaltung der Vendor Insights-Ressourcen

`AWSVendorInsightsVendorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSVendorInsightsVendorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 19. Oktober 2023, 01:41 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:CreateDataSource",
        "vendor-insights:UpdateDataSource",
        "vendor-insights:DeleteDataSource",
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:CreateSecurityProfile",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:AssociateDataSource",
        "vendor-insights:DisassociateDataSource",
        "vendor-insights:UpdateSecurityProfile",
        "vendor-insights:ActivateSecurityProfile",
        "vendor-insights:DeactivateSecurityProfile",
        "vendor-insights:UpdateSecurityProfileSnapshotCreationConfiguration",
        "vendor-insights:UpdateSecurityProfileSnapshotReleaseConfiguration",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:TagResource",
        "vendor-insights:UntagResource",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "aws-marketplace:AcceptAgreementApprovalRequest",
        "aws-marketplace:RejectAgreementApprovalRequest",
        "aws-marketplace:GetAgreementApprovalRequest",
        "aws-marketplace:ListAgreementApprovalRequests",
        "aws-marketplace:CancelAgreement",
        "aws-marketplace:SearchAgreements"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:AgreementType" : "VendorInsightsAgreement"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVendorInsightsVendorReadOnly

Beschreibung: Bietet Lesezugriff zum Anzeigen der Vendor Insights-Ressourcen

`AWSVendorInsightsVendorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSVendorInsightsVendorReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 26. Juli 2022, 15:05 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 00:54 UTC
- ARN: `arn:aws:iam::aws:policy/AWSVendorInsightsVendorReadOnly`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:DescribeEntity",
      "Resource" : "arn:aws:aws-marketplace:*:*:*/SaaSProduct/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "aws-marketplace:ListEntities",
      "Resource" : "*"
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "vendor-insights:GetDataSource",
        "vendor-insights:ListDataSources",
        "vendor-insights:ListSecurityProfiles",
        "vendor-insights:GetSecurityProfile",
        "vendor-insights:GetSecurityProfileSnapshot",
        "vendor-insights:ListSecurityProfileSnapshots",
        "vendor-insights:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource" : "arn:aws:artifact:*::report/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVpcLatticeServiceRolePolicy

Beschreibung: Ermöglicht VPC Lattice, in Ihrem Namen auf AWS Ressourcen zuzugreifen.

`AWSVpcLatticeServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2022, 20:47 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 14:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVpcLatticeServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/VpcLattice"
        }
      }
    },
    {
```

```
      "Sid" : "VpcLatticeDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeCreateNetworkInterfaceWithSubnetAndSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VpcLatticeTagNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
```

```
        }
      }
    },
    {
      "Sid" : "VpcLatticeMutateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VpcLatticeModifyNetworkInterfaceActionsIpAddressActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VpcLatticeManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VpcLatticeAssociateHostedZoneToVpc",
```

```
      "Effect" : "Allow",
      "Action" : [
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCS2SVpnServiceRolePolicy

Beschreibung: Erlauben Sie Site-to-Site VPN, Ressourcen im Zusammenhang mit Ihren VPN-Verbindungen zu erstellen und zu verwalten.

`AWSVPCS2SVpnServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. August 2019, 14:13 Uhr UTC
- Bearbeitete Zeit: 15. Mai 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCS2SVpnServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "0",
      "Effect" : "Allow",
      "Action" : [
        "acm:ExportCertificate",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VpnConnectionSecretsManagement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringEquals" : {
          "secretsmanager:ResourceTag/aws:secretsmanager:owningService" : "s2svpn",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "VpnConnectionSecretsCreation",
      "Effect" : "Allow",
      "Action" : "secretsmanager:CreateSecret",
      "Resource" : "arn:aws:secretsmanager:*:*:secret:s2svpn!*",
      "Condition" : {
        "StringLike" : {
          "secretsmanager:Name" : "s2svpn!*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCTransitGatewayServiceRolePolicy

Beschreibung: Erlauben Sie VPC Transit Gateway, die erforderlichen Ressourcen für Ihre Transit Gateway Gateway-VPC-Anhänge zu erstellen und zu verwalten.

`AWSVPCTransitGatewayServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2018, 16:21 UTC
- Bearbeitete Zeit: 15. April 2021, 16:31 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCTransitGatewayServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AssignIpv6Addresses",
        "ec2:UnAssignIpv6Addresses"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Sid" : "0"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSVPCVerifiedAccessServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung des AWS Verified Access-Dienstes zur Bereitstellung von Endpunkten in Ihrem Namen

`AWSVPCVerifiedAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 03:35 UTC
- Bearbeitete Zeit: 17. November 2023, 21:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSVPCVerifiedAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VerifiedAccessRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleModifyNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "VerifiedAccessRoleNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "VerifiedAccessRoleTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/VerifiedAccessManaged" : "true"
        }
      }
    },
    {
      "Sid" : "VerifiedAccessRoleTaggingActions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS WAF über die AWS-Managementkonsole. Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten und Aktualisieren von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway-REST APIs und -Stages, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von Regionen gewährt, die innerhalb des Kontos aktiviert sind.

`AWSWAFConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSWAFConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. April 2020, 18:38 UTC

- Zeit bearbeitet: 19. November 2025, 02:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
```

```
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution",
        "cloudfront:UpdateDistribution",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant",
        "cloudfront:AssociateDistributionTenantWebACL",
        "cloudfront:DisassociateDistributionTenantWebACL"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
```

```
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
```

```
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : "pricingplanmanager:ListSubscriptions",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF über die. AWS-Managementkonsole Beachten Sie, dass diese Richtlinie auch Berechtigungen zum Auflisten von CloudFront Amazon-Distributionen, Berechtigungen zum Anzeigen von Load Balancern auf AWS Elastic Load Balancing, Berechtigungen zum Anzeigen von Amazon API Gateway-REST APIs und -Stages, Berechtigungen zum Auflisten und Anzeigen von CloudWatch Amazon-Metriken sowie Berechtigungen zum Anzeigen von Regionen gewährt, die innerhalb des Kontos aktiviert sind.

`AWSWAFConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSWAFConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. April 2020, 18:43 UTC
- Zeit bearbeitet: 19. November 2025, 02:34 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
```

```
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf:*:*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
```

```
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowEC2DescribeRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForCloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionConfig",
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
```

```
      "Sid" : "AllowListActionsForCloudFront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistributionTenant"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution-tenant/*"
    },
    {
      "Sid" : "AllowListActionsForCloudFrontTenant",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:ListDistributionTenants",
        "cloudfront:ListDistributionTenantsByCustomization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : "arn:aws:apigateway:*::/*"
    },
    {
      "Sid" : "AllowListActionsForAppSync",
      "Effect" : "Allow",
```

```
      "Action" : [
        "appsync:ListGraphqlApis",
        "appsync:ListApis"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListUserPools",
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstances",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListApps",
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowS3ListAllMyBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListActionForFirehoseStream",
      "Effect" : "Allow",
      "Action" : [
        "firehose:ListDeliveryStreams"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForPricing",
      "Effect" : "Allow",
      "Action" : [
        "pricing:ListPriceLists",
        "pricing:GetPriceListFileUrl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowMarketplaceViewSubscriptions",
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogQueryActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:DescribeQueryDefinitions",
        "logs:GetQueryResults"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:aws-waf-logs-*"
    },
    {
      "Sid" : "AllowListActionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:GetSubscription"
      ],
```

```
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    },
    {
      "Sid" : "AllowListActionsForRoute53",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListHostedZones",
        "route53:GetHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowListSubscriptionsForPricingPlanManager",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:ListSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFFullAccess

Beschreibung: Bietet vollen Zugriff auf AWS WAF-Aktionen.

`AWSWAFFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSWAFFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Oktober 2015, 20:44 UTC
- Bearbeitete Zeit: 5. Mai 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFFullAccess`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowUseOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:*",
        "waf-regional:*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
```

```
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowUseOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:*"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowDisassociateWebACL",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:DisassociateWebACL"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForALB",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:SetWebAcl"
      ],
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
    },
    {
      "Sid" : "AllowActionsForAPIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:SetWebACL"
      ],
      "Resource" : "arn:aws:apigateway:*::/restapis/*/stages/*"
    },
    {
      "Sid" : "AllowActionsForAppSync",
      "Effect" : "Allow",
      "Action" : [
        "appsync:SetWebACL"
      ],
      "Resource" : "arn:aws:appsync:*:*:apis/*"
    },
    {
      "Sid" : "AllowActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:AssociateWebACL",
        "cognito-idp:DisassociateWebACL",
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AllowActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:AssociateWebAcl",
        "apprunner:DisassociateWebAcl",
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateVerifiedAccessInstanceWebAcl",
        "ec2:DisassociateVerifiedAccessInstanceWebAcl",
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:AssociateWebACL",
        "amplify:DisassociateWebACL",
```

```
        "amplify:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogGroupDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLogDeliverySubscription",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForS3Bucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "GrantLogDeliveryPermissionForCloudWatchLogGroup",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWAFReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS WAF-Aktionen.

`AWSWAFReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSWAFReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Oktober 2015, 20:43 UTC
- Bearbeitete Zeit: 5. Mai 2025, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWAFReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyOfAWSWAFClassic",
      "Effect" : "Allow",
      "Action" : [
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*"
      ],
      "Resource" : [
        "arn:aws:waf::*:bytematchset/*",
        "arn:aws:waf::*:ipset/*",
        "arn:aws:waf::*:ratebasedrule/*",
        "arn:aws:waf::*:rule/*",
        "arn:aws:waf::*:sizeconstraintset/*",
        "arn:aws:waf::*:sqlinjectionset/*",
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf::*:xssmatchset/*",
        "arn:aws:waf::*:regexmatch/*",
        "arn:aws:waf::*:regexpatternset/*",
        "arn:aws:waf::*:geomatchset/*",
        "arn:aws:waf::*:rulegroup/*",
        "arn:aws:waf::*:changetoken/*",
        "arn:aws:waf-regional:*:*:bytematchset/*",
        "arn:aws:waf-regional:*:*:ipset/*",
        "arn:aws:waf-regional:*:*:ratebasedrule/*",
        "arn:aws:waf-regional:*:*:rule/*",
        "arn:aws:waf-regional:*:*:sizeconstraintset/*",
        "arn:aws:waf-regional:*:*:sqlinjectionset/*",
```

```
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:xssmatchset/*",
        "arn:aws:waf-regional:*:*:regexmatch/*",
        "arn:aws:waf-regional:*:*:regexpatternset/*",
        "arn:aws:waf-regional:*:*:geomatchset/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:changetoken/*"
      ]
    },
    {
      "Sid" : "AllowWAFClassicGetWebACLForResource",
      "Effect" : "Allow",
      "Action" : [
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:waf-regional:*:*:*/*"
    },
    {
      "Sid" : "AllowReadOnlyOfAWSWAF",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:Get*",
        "wafv2:List*",
        "wafv2:Describe*",
        "wafv2:CheckCapacity"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:*/webacl/*/*",
        "arn:aws:wafv2:*:*:*/ipset/*/*",
        "arn:aws:wafv2:*:*:*/managedruleset/*/*",
        "arn:aws:wafv2:*:*:*/rulegroup/*/*",
        "arn:aws:wafv2:*:*:*/regexpatternset/*/*"
      ]
    },
    {
      "Sid" : "AllowGetActionForCognito",
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:GetWebACLForResource"
      ],
      "Resource" : "arn:aws:cognito-idp:*:*:userpool/*"
    },
    {
      "Sid" : "AllowListActionsForCognito",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cognito-idp:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:DescribeWebAclForService"
      ],
      "Resource" : "arn:aws:apprunner:*:*:service/*/*"
    },
    {
      "Sid" : "AllowListActionsForAppRunner",
      "Effect" : "Allow",
      "Action" : [
        "apprunner:ListServices",
        "apprunner:ListAssociatedServicesForWebAcl"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetVerifiedAccessInstanceWebAcl"
      ],
      "Resource" : "arn:aws:ec2:*:*:verified-access-instance/*"
    },
    {
      "Sid" : "AllowListActionsForAVA",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGetActionForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:GetWebACLForResource"
```

```
      ],
      "Resource" : "arn:aws:amplify:*:*:apps/*"
    },
    {
      "Sid" : "AllowListActionsForAmplify",
      "Effect" : "Allow",
      "Action" : [
        "amplify:ListResourcesForWebACL"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWellArchitectedDiscoveryServiceRolePolicy

Beschreibung: Ermöglicht WellArchitected den Zugriff auf AWS Dienste und Ressourcen, die sich auf WellArchitected Ressourcen im Namen von Kunden beziehen.

`AWSWellArchitectedDiscoveryServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. April 2023, 18:36 UTC

- Bearbeitete Zeit: 26. April 2023, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedDiscoveryServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "trustedadvisor:DescribeChecks",
        "trustedadvisor:DescribeCheckItems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "resource-groups:ListGroupResources",
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:ListAssociatedResources",
        "servicecatalog:GetApplication",
        "servicecatalog:CreateAttributeGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:AssociateAttributeGroup",
        "servicecatalog:DisassociateAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/applications/*",
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "servicecatalog:UpdateAttributeGroup",
        "servicecatalog:DeleteAttributeGroup"
      ],
      "Resource" : [
        "arn:*:servicecatalog:*:*:/attribute-groups/AWS_WellArchitected-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWellArchitectedOrganizationsServiceRolePolicy

Beschreibung: Ermöglicht Well-Architected, in Ihrem Namen auf Organizations zuzugreifen.

`AWSWellArchitectedOrganizationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Juni 2022, 17:15 UTC
- Bearbeitete Zeit: 25. Juli 2022, 18:03 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSWellArchitectedOrganizationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSWickrFullAccess

Beschreibung: Diese Richtlinie gewährt dem Wickr-Dienst vollständige Administratorrechte, einschließlich der Wickr-Verwaltungsfunktionen unter. AWS-Managementkonsole

`AWSWickrFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSWickrFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 20:36 UTC
- Zeit bearbeitet: 27. November 2022, 20:36 UTC
- ARN: `arn:aws:iam::aws:policy/AWSWickrFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "wickr:*",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur gemeinsamen Nutzung von X-Ray-Traces

`AWSXrayCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSXrayCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:46 UTC
- Zeit bearbeitet: 27. November 2022, 13:46 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
```

```
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXRayDaemonWriteAccess

Beschreibung: Erlaubt dem AWS X-Ray-Daemon, rohe Trace-Segmentdaten an die API des Dienstes weiterzuleiten und Sampling-Daten (Regeln, Ziele usw.) abzurufen, die vom X-Ray-SDK verwendet werden können.

`AWSXRayDaemonWriteAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSXRayDaemonWriteAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. August 2018, 23:00 Uhr UTC
- Bearbeitete Zeit: 13. Februar 2024, 21:58 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXRayDaemonWriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayFullAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie mit vollem Zugriff

`AWSXrayFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSXrayFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:30 Uhr UTC
- Bearbeitete Zeit: 11. April 2024, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayFullAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "xray:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayReadOnlyAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie nur zum Lesen

`AWSXrayReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSXrayReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:27 UTC
- Bearbeitete Zeit: 14. Februar 2024, 00:35 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSXrayReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "xray:BatchGetTraces",
        "xray:BatchGetTraceSummaryById",
        "xray:GetDistinctTraceGraphs",
        "xray:GetServiceGraph",
        "xray:GetTraceGraph",
        "xray:GetTraceSummaries",
        "xray:GetGroups",
        "xray:GetGroup",
        "xray:ListTagsForResource",
        "xray:ListResourcePolicies",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetInsightSummaries",
        "xray:GetInsight",
        "xray:GetInsightEvents",
        "xray:GetInsightImpactGraph"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSXrayWriteOnlyAccess

Beschreibung: Verwaltete AWS X-Ray-Richtlinie nur zum Schreiben

`AWSXrayWriteOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `AWSXrayWriteOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2016, 18:19 Uhr UTC
- Bearbeitete Zeit: 28. August 2018, 23:03 UTC
- ARN: `arn:aws:iam::aws:policy/AWSXrayWriteOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSZonalAutoshiftPracticeRunSLRPolicy

Beschreibung: Bietet administrativen Zugriff auf Übungsläufe in ARC-Zonenschichten sowie Zugriff auf CloudWatch Alarmstatus zur Überwachung von Übungsläufen.

`AWSZonalAutoshiftPracticeRunSLRPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2023, 17:34 UTC
- Bearbeitete Zeit: 30. Juni 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZonalAutoshiftPracticeRunSLRPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MonitoringPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "health:DescribeEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoshiftPracticeCheckPermissions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroups"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ZonalShiftManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:CancelZonalShift",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:StartZonalShift",
        "arc-zonal-shift:UpdateZonalShift"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

AWSZoneGroupAccessManagementServiceRolePolicy

Beschreibung: Bietet schreibgeschützten Zugriff auf die Informationen, die zur Unterstützung der Verwaltung von Zonengruppen für Organisationen APIs erforderlich sind.

`AWSZoneGroupAccessManagementServiceRolePolicy`ist AWS eine verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Juli 2025, 19:07 UTC

- Bearbeitete Zeit: 1. Juli 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/AWSZoneGroupAccessManagementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BatchServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf den AWS Batch-Service zur Verwaltung der erforderlichen Ressourcen, einschließlich Amazon EC2 - und Amazon ECS-Ressourcen.

`BatchServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. März 2021, 06:55 UTC
- Bearbeitete Zeit: 5. Dezember 2023, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BatchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "AWSBatchPolicyStatement1",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeImages",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeSpotInstanceRequests",
        "ec2:DescribeSpotFleetInstances",
        "ec2:DescribeSpotFleetRequests",
        "ec2:DescribeSpotPriceHistory",
        "ec2:DescribeSpotFleetRequestHistory",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:RequestSpotFleet",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeScalingActivities",
        "eks:DescribeCluster",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListTaskDefinitionFamilies",
        "ecs:ListTaskDefinitions",
        "ecs:ListTasks",
        "ecs:DeregisterTaskDefinition",
        "ecs:TagResource",
        "ecs:ListAccountSettings",
        "logs:DescribeLogGroups",
        "iam:GetInstanceProfile",
        "iam:GetRole"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AWSBatchPolicyStatement2",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement3",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/batch/job*:log-stream:*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement4",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateOrUpdateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement5",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn",
            "ecs-tasks.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement6",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "spot.amazonaws.com",
            "spotfleet.amazonaws.com",
            "autoscaling.amazonaws.com",
            "ecs.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement7",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement8",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:CancelSpotFleetRequests",
        "ec2:ModifySpotFleetRequest",
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement9",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateLaunchConfiguration",
        "autoscaling:DeleteLaunchConfiguration"
      ],
      "Resource" :
 "arn:aws:autoscaling:*:*:launchConfiguration:*:launchConfigurationName/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement10",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CreateAutoScalingGroup",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SetDesiredCapacity",
        "autoscaling:DeleteAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:PutNotificationConfiguration",
        "autoscaling:TerminateInstanceInAutoScalingGroup"
      ],
      "Resource" : "arn:aws:autoscaling:*:*:autoScalingGroup:*:autoScalingGroupName/
AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement11",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DeleteCluster",
        "ecs:DeregisterContainerInstance",
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:cluster/AWSBatch*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement12",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ecs:RunTask",
        "ecs:StartTask",
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task-definition/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement13",
      "Effect" : "Allow",
      "Action" : [
        "ecs:StopTask"
      ],
      "Resource" : "arn:aws:ecs:*:*:task/*/*"
    },
    {
      "Sid" : "AWSBatchPolicyStatement14",
      "Effect" : "Allow",
      "Action" : [
        "ecs:CreateCluster",
        "ecs:RegisterTaskDefinition"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement15",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:placement-group/*",
        "arn:aws:ec2:*:*:capacity-reservation/*",
```

```
        "arn:aws:ec2:*:*:elastic-gpu/*",
        "arn:aws:elastic-inference:*:*:elastic-inference-accelerator/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    },
    {
      "Sid" : "AWSBatchPolicyStatement16",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AWSBatchServiceTag" : "false"
        }
      }
    },
    {
      "Sid" : "AWSBatchPolicyStatement17",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances",
            "CreateLaunchTemplate",
            "RequestSpotFleet"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BedrockAgentCoreFullAccess

Beschreibung: Bietet vollen Zugriff auf Bedrock AgentCore sowie eingeschränkten Zugriff auf zugehörige Dienste

`BedrockAgentCoreFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `BedrockAgentCoreFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Juli 2025, 13:37 UTC
- Bearbeitete Zeit: 2. Dezember 2025, 13:34 UTC
- ARN: `arn:aws:iam::aws:policy/BedrockAgentCoreFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAgentCoreFullAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock-agentcore:*"
      ],
      "Resource" : "arn:aws:bedrock-agentcore:*:*:*"
    },
    {
      "Sid" : "IAMListAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:role/*"
    },
    {
      "Sid" : "BedrockAgentCorePassRoleAccess",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*BedrockAgentCore*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:bedrock-agentcore*"
    },
    {
      "Sid" : "BedrockAgentCoreKMSReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:DescribeKey"
```

```
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:ListGrants"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "bedrock-agentcore.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreKMSGrantsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "kms:GrantConstraintType" : "EncryptionContextSubset"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : [
            "bedrock-agentcore.*.amazonaws.com"
          ],
          "kms:EncryptionContext:aws:bedrock-agentcore-gateway:arn" : "arn:aws:bedrock-
agentcore:*:*:gateway/*"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "GenerateDataKey"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-gateway-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "bedrock-agentcore.amazonaws.com",
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreGatewayLambdaAccess",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:*"
      ]
    },
    {
      "Sid" : "BedrockAgentCoreGatewayApiGateway",
```

```
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis/*/stages/*/exports/*"
      ]
    },
    {
      "Sid" : "LoggingAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "ObservabilityReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "oam:ListSinks",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
```

```
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval",
        "logs:DescribeLogGroups",
        "logs:StartLiveTail",
        "logs:StopLiveTail"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchXRayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSegmentDestination",
        "xray:UpdateTraceSegmentDestination",
        "xray:GetIndexingRules",
        "xray:UpdateIndexingRule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransactionSearchLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "TransactionSearchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TransactionSearchApplicationSignalsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:StartDiscovery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CreateBedrockAgentCoreNetworkServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/network.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreNetwork",
      "Condition" : {
```

```
        "StringEquals" : {
          "iam:AWSServiceName" : "network.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CreateBedrockAgentCoreRuntimeIdentityServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/runtime-identity.bedrock-
agentcore.amazonaws.com/AWSServiceRoleForBedrockAgentCoreRuntimeIdentity",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "runtime-identity.bedrock-agentcore.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3WriteAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::bedrock-agentcore-runtime-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeS3ListAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockAgentCoreRuntimeECRAccess",
      "Effect" : "Allow",
      "Action" : [
        "ecr:DescribeRepositories",
        "ecr:DescribeImages",
        "ecr:ListImages"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogCreate",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/bedrock-agentcore/evaluations/*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationCloudWatchLogIndexAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutIndexPolicy",
        "logs:DescribeIndexPolicies"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:aws/spans",
        "arn:aws:logs:*:*:log-group:aws/spans:*"
      ]
    },
    {
      "Sid" : "AgentCoreEvaluationBedrockInvokeAccess",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:inference-profile/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BedrockAgentCoreNetworkServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf andere AWS Serviceressourcen, die für die Ausführung von Amazon Bedrock AgentCore im VPC-Modus erforderlich sind

`BedrockAgentCoreNetworkServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. September 2025, 22:04 UTC
- Bearbeitete Zeit: 19. September 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreNetworkServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowCreateEniInAnySubnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
```

```
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Sid" : "AllowCreateEniWithSecurityGroups",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "AllowCreateEniWithBedrockManagedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonBedrockAgentCoreManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagEniOnCreate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "AllowManageEniWhenBedrockManaged",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:CreateNetworkInterfacePermission"
      ],
```

```
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonBedrockAgentCoreManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGetSecurityGroupsForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:GetSecurityGroupsForVPC"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Sid" : "AllowDescribeNetworkingResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BedrockAgentCoreRuntimeIdentityServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf Identitäts- und Tokenverwaltungsressourcen, die für die Authentifizierung und Autorisierung von Amazon Bedrock AgentCore Runtime erforderlich sind.

`BedrockAgentCoreRuntimeIdentityServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 11. Oktober 2025, 01:04 UTC
- Bearbeitete Zeit: 11. Oktober 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BedrockAgentCoreRuntimeIdentityServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Sid" : "AllowWorkloadIdentityAccess",
    "Effect" : "Allow",
    "Action" : [
      "bedrock-agentcore:GetWorkloadAccessToken",
      "bedrock-agentcore:GetWorkloadAccessTokenForJWT",
      "bedrock-agentcore:GetWorkloadAccessTokenForUserId"
    ],
    "Resource" : [
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default",
      "arn:aws:bedrock-agentcore:*:*:workload-identity-directory/default/workload-
identity/*"
```

```
    ]
  }
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Billing

Beschreibung: Erteilt Berechtigungen für die Abrechnung und das Kostenmanagement. Dazu gehören das Anzeigen der Kontonutzung sowie das Anzeigen und Ändern von Budgets und Zahlungsmethoden.

`Billing`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `Billing` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:33 Uhr UTC
- Bearbeitete Zeit: 18. November 2025, 21:49 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/Billing`

Version der Richtlinie

Richtlinienversion: v17 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VisualEditor0",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "aws-portal:*Billing",
        "aws-portal:*PaymentMethods",
        "aws-portal:*Usage",
        "billing:CreateBillingView",
        "billing:DeleteBillingView",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:PutContractInformation",
        "billing:RedeemCredits",
        "billing:GetResourcePolicy",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billing:TagResource",
        "billing:UntagResource",
        "billing:UpdateBillingPreferences",
        "billing:UpdateBillingView",
        "billing:UpdateIAMAccessPreference",
        "budgets:CreateBudgetAction",
        "budgets:DeleteBudgetAction",
        "budgets:DescribeBudgetActionsForBudget",
        "budgets:DescribeBudgetAction",
        "budgets:DescribeBudgetActionsForAccount",
        "budgets:DescribeBudgetActionHistories",
        "budgets:ExecuteBudgetAction",
        "budgets:ModifyBudget",
```

```
        "budgets:UpdateBudgetAction",
        "budgets:ViewBudget",
        "ce:CreateCostCategoryDefinition",
        "ce:CreateNotificationSubscription",
        "ce:CreateReport",
        "ce:DeleteCostCategoryDefinition",
        "ce:DeleteNotificationSubscription",
        "ce:DeleteReport",
        "ce:DescribeCostCategoryDefinition",
        "ce:GetCostAndUsage",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListTagsForResource",
        "ce:TagResource",
        "ce:UpdateCostAllocationTagsStatus",
        "ce:UpdateNotificationSubscription",
        "ce:UpdatePreferences",
        "ce:UpdateReport",
        "ce:UpdateCostCategoryDefinition",
        "ce:UntagResource",
        "ce:StartCostAllocationTagBackfill",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:GetTags",
        "ce:GetDimensionValues",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:DeleteReportDefinition",
        "cur:DescribeReportDefinitions",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "cur:ModifyReportDefinition",
        "cur:PutClassicReportPreferences",
        "cur:PutReportDefinition",
        "cur:ValidateReportDestination",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:PutFreeTierAlertPreference",
        "invoicing:BatchGetInvoiceProfile",
        "invoicing:CreateInvoiceUnit",
        "invoicing:DeleteInvoiceUnit",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:GetInvoiceUnit",
```

```
        "invoicing:GetInvoiceCorrection",
        "invoicing:ListInvoiceSummaries",
        "invoicing:ListInvoiceUnits",
        "invoicing:CreateProcurementPortalPreference",
        "invoicing:GetProcurementPortalPreference",
        "invoicing:PutProcurementPortalPreference",
        "invoicing:UpdateProcurementPortalPreferenceStatus",
        "invoicing:ListProcurementPortalPreferences",
        "invoicing:DeleteProcurementPortalPreference",
        "invoicing:ListTagsForResource",
        "invoicing:ListInvoiceCorrections",
        "invoicing:StartInvoiceCorrection",
        "invoicing:PutInvoiceEmailDeliveryPreferences",
        "invoicing:TagResource",
        "invoicing:UntagResource",
        "invoicing:UpdateInvoiceUnit",
        "mapcredits:ListQuarterSpend",
        "mapcredits:ListAssociatedPrograms",
        "mapcredits:ListQuarterCredits",
        "payments:CreateFinancingApplication",
        "payments:CreatePaymentInstrument",
        "payments:DeletePaymentInstrument",
        "payments:GetFinancingApplication",
        "payments:GetFinancingLine",
        "payments:GetFinancingLineWithdrawal",
        "payments:GetFinancingOption",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListFinancingApplications",
        "payments:ListFinancingLines",
        "payments:ListFinancingLineWithdrawals",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "payments:ListPaymentInstruments",
        "payments:MakePayment",
        "payments:TagResource",
        "payments:UntagResource",
        "payments:UpdateFinancingApplication",
        "payments:UpdatePaymentInstrument",
        "payments:UpdatePaymentPreferences",
        "pricing:DescribeServices",
        "purchase-orders:AddPurchaseOrder",
```

```
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:TagResource",
        "purchase-orders:UntagResource",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus",
        "purchase-orders:ViewPurchaseOrders",
        "support:CreateCase",
        "support:AddAttachmentsToSet",
        "sustainability:GetCarbonFootprintSummary",
        "tax:BatchPutTaxRegistration",
        "tax:DeleteTaxRegistration",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "tax:PutTaxInheritance",
        "tax:PutTaxInterview",
        "tax:PutTaxRegistration",
        "tax:UpdateExemptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

BudgetsServiceRolePolicy

Beschreibung: Ermöglicht Budgets, den Zugriff auf Abrechnungsansichten zu überprüfen, die über Kontogrenzen hinweg gemeinsam genutzt werden.

`BudgetsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. Juli 2025, 21:07 UTC
- Bearbeitete Zeit: 30. Juli 2025, 21:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/BudgetsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "billing:GetBillingViewData"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CertificateManagerServiceRolePolicy

Beschreibung: Amazon Certificate Manager Service Rollenrichtlinie

`CertificateManagerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Juni 2020, 17:56 Uhr UTC
- Bearbeitete Zeit: 25. Juni 2020, 17:56 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CertificateManagerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ClientVPNServiceConnectionsRolePolicy

Beschreibung: Richtlinie, mit der AWS Client VPN Ihre Client-VPN-Endpunktverbindungen verwalten kann.

`ClientVPNServiceConnectionsRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. August 2020, 19:48 UTC
- Bearbeitete Zeit: 12. August 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceConnectionsRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:InvokeFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AWSClientVPN-*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ClientVPNServiceRolePolicy

Beschreibung: Richtlinie zur Aktivierung von AWS Client VPN zur Verwaltung Ihrer Client-VPN-Endpunkte.

`ClientVPNServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Dezember 2018, 21:20 Uhr UTC
- Bearbeitete Zeit: 12. August 2020, 19:39 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ClientVPNServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeInternetGateways",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeAccountAttributes",
        "ds:AuthorizeApplication",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:UnauthorizeApplication",
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "acm:GetCertificate",
        "acm:DescribeCertificate",
        "iam:GetSAMLProvider",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFormationStackSetsOrgAdminServiceRolePolicy

Beschreibung: Servicerolle für CloudFormation StackSets (Unternehmens-Hauptkonto)

`CloudFormationStackSetsOrgAdminServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Dezember 2019, 00:20 Uhr UTC
- Bearbeitete Zeit: 10. Dezember 2019, 00:20 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgAdminServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsAWSOrganizationsReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowAssumeRoleInMemberAccounts",
      "Effect" : "Allow",
      "Action" : "sts:AssumeRole",
      "Resource" : "arn:aws:iam::*:role/stacksets-exec-*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFormationStackSetsOrgMemberServiceRolePolicy

Beschreibung: Servicerolle für CloudFormation StackSets (Mitgliedskonto der Organisation)

`CloudFormationStackSetsOrgMemberServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. Dezember 2019, 23:52 Uhr UTC
- Bearbeitete Zeit: 9. Dezember 2019, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudFormationStackSetsOrgMemberServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ]
    },
    {
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/stacksets-exec-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/AdministratorAccess"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFrontFullAccess

Beschreibung: Bietet vollen Zugriff auf die CloudFront Konsole sowie die Möglichkeit, Amazon S3 S3-Buckets über die AWS-Managementkonsole aufzulisten.

`CloudFrontFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudFrontFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 18. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontFullAccess`

Version der Richtlinie

Richtlinienversion: v10 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfflistbuckets",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "cffullaccess",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:*",
        "cloudfront-keyvaluestore:*",
        "iam:ListServerCertificates",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "wafv2:CreateWebACL",
        "kinesis:ListStreams",
        "ec2:DescribeInstances",
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:CreateSubscription"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cfrequestcertificate",
      "Effect" : "Allow",
      "Action" : [
        "acm:RequestCertificate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "cloudfront.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "cffdescribestream",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kinesis:DescribeStream"
      ],
      "Resource" : "arn:aws:kinesis:*:*:*"
    },
    {
      "Sid" : "cfflistroles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "arn:aws:iam::*:*"
    },
    {
      "Sid" : "ppmFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "pricingplanmanager:AssociateResourcesToSubscription",
        "pricingplanmanager:CancelSubscription",
        "pricingplanmanager:CancelSubscriptionChange",
        "pricingplanmanager:DisassociateResourcesFromSubscription",
        "pricingplanmanager:GetSubscription",
        "pricingplanmanager:UpdateSubscription"
      ],
      "Resource" : "arn:aws:pricingplanmanager::*:subscription:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudFrontReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf Informationen zur CloudFront Distributionskonfiguration und Listenverteilungen über die AWS-Managementkonsole.

`CloudFrontReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudFrontReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 18. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "cfReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudfront:Describe*",
        "cloudfront:Get*",
```

```
        "cloudfront:List*",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "iam:ListServerCertificates",
        "route53:List*",
        "waf:ListWebACLs",
        "waf:GetWebACL",
        "wafv2:ListWebACLs",
        "wafv2:GetWebACL",
        "ec2:DescribeIpamPools",
        "ec2:GetIpamPoolCidrs",
        "pricingplanmanager:ListSubscriptions",
        "pricingplanmanager:GetSubscription"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudHSMServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS Ressourcen, die von CloudHSM verwendet oder verwaltet werden

`CloudHSMServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 6. November 2017, 19:12 UTC
- Zeit bearbeitet: 6. November 2017, 19:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudHSMServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudSearchFullAccess

Beschreibung: Bietet vollen Zugriff auf den CloudSearch Amazon-Konfigurationsservice.

`CloudSearchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudSearchFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:*"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudSearchReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den CloudSearch Amazon-Konfigurationsservice.

`CloudSearchReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudSearchReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:39 UTC
- ARN: `arn:aws:iam::aws:policy/CloudSearchReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudsearch:Describe*",
        "cloudsearch:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudTrailEventContext

Beschreibung: Diese dienstbezogene Rolle ermöglicht das CloudTrail Abrufen und Hinzufügen von Ressourcen-Tags zu den CloudTrail Ereignissen des Ressourcenbesitzers.

`CloudTrailEventContext`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Mai 2025, 13:52 UTC
- Bearbeitete Zeit: 15. Mai 2025, 13:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailEventContext`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailEventContextPermissionForTag",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleCreation",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : "aws.tag"
```

```
        },
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:detail-type" : "Tag Change on Resource",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleWrite",
      "Effect" : "Allow",
      "Action" : [
        "events:PutTargets",
        "events:DeleteRule",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*",
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}",
          "events:ManagedBy" : "context.cloudtrail.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowEventBridgeRuleRead",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:ListTargetsByRule"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:creatorAccount" : "${aws:PrincipalAccount}"
        }
      },
      "Resource" : "arn:aws:events:*:*:rule/CloudTrailEventContext*"
    },
    {
      "Sid" : "AllowEventBridgeRuleList",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudTrailServiceRolePolicy

Beschreibung: Berechtigungsrichtlinie für CloudTrail ServiceLinkedRole

`CloudTrailServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Oktober 2018, 21:21 Uhr UTC
- Bearbeitete Zeit: 27. November 2023, 01:18 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudTrailServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudTrailFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsDelegatedAdminAccess",
      "Effect" : "Allow",
      "Action" : "organizations:ListDelegatedAdministrators",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : [
            "cloudtrail.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "DeleteTableAccess",
      "Effect" : "Allow",
      "Action" : "glue:DeleteTable",
      "Resource" : [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/aws:cloudtrail",
        "arn:*:glue:*:*:table/aws:cloudtrail/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DeregisterResourceAccess",
      "Effect" : "Allow",
      "Action" : "lakeformation:DeregisterResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatch-CrossAccountAccess

Beschreibung: Ermöglicht CloudWatch die Übernahme von CrossAccountSharing Rollen in Remote-Konten im Namen des aktuellen Kontos, um Daten konto CloudWatch - und regionsübergreifend anzuzeigen

`CloudWatch-CrossAccountAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Juli 2019, 09:59 Uhr UTC
- Bearbeitete Zeit: 23. Juli 2019, 09:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatch-CrossAccountAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/CloudWatch-CrossAccountSharing*"
      ],
      "Effect" : "Allow"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchActionsEC2Access

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Alarme und Messwerte sowie EC2 Metadaten. Bietet Zugriff auf Stop-, Terminate- und EC2 Reboot-Instances.

`CloudWatchActionsEC2Access`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchActionsEC2Access` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Juli 2015, 00:00 UTC
- Bearbeitete Zeit: 7. Juli 2015, 00:00 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchActionsEC2Access`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Describe*",
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAgentAdminPolicy

Beschreibung: Für die Verwendung sind vollständige Berechtigungen erforderlich AmazonCloudWatchAgent.

`CloudWatchAgentAdminPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchAgentAdminPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 00:52 UTC
- Zeit bearbeitet: 5. Februar 2024, 20:59 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentAdminPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAgentServerPolicy

Beschreibung: Für die Verwendung AmazonCloudWatchAgent auf Servern sind Berechtigungen erforderlich

`CloudWatchAgentServerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchAgentServerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2018, 01:06 UTC
- Bearbeitete Zeit: 6. Februar 2024, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CWACloudWatchServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "ec2:DescribeVolumes",
        "ec2:DescribeTags",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWASSMServerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationInsightsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Application Insights und die erforderlichen Abhängigkeiten.

`CloudWatchApplicationInsightsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchApplicationInsightsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. November 2020, 18:44 Uhr UTC
- Bearbeitete Zeit: 25. Januar 2022, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "applicationinsights:*",
```

```
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "sqs:ListQueues",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "autoscaling:DescribeAutoScalingGroups",
        "lambda:ListFunctions",
        "dynamodb:ListTables",
        "s3:ListAllMyBuckets",
        "sns:ListTopics",
        "states:ListStateMachines",
        "apigateway:GET",
        "ecs:ListClusters",
        "ecs:DescribeTaskDefinition",
        "ecs:ListServices",
        "ecs:ListTasks",
        "eks:ListClusters",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationInsightsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Application Insights.

`CloudWatchApplicationInsightsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchApplicationInsightsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. November 2020, 18:48 Uhr UTC
- Bearbeitete Zeit: 24. November 2020, 18:48 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationInsightsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:Describe*",
        "applicationinsights:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudwatchApplicationInsightsServiceLinkedRolePolicy

Beschreibung: Richtlinie für verknüpfte Rollen mit dem Cloudwatch Application Insights Service

`CloudwatchApplicationInsightsServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2018, 16:22 UTC
- Bearbeitete Zeit: 25. Juli 2024, 16:24 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudwatchApplicationInsightsServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v25 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:PutAnomalyDetector",
        "cloudwatch:DeleteAnomalyDetector",
        "cloudwatch:DescribeAnomalyDetectors"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridge",
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:CreateStack",
        "cloudFormation:UpdateStack",
        "cloudFormation:DeleteStack",
        "cloudFormation:DescribeStackResources",
        "cloudFormation:UpdateTerminationProtection"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "CloudFormationStacks",
      "Effect" : "Allow",
      "Action" : [
        "cloudFormation:DescribeStacks",
        "cloudFormation:ListStackResources",
        "cloudFormation:ListStacks"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ResourceGroups",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources",
        "resource-groups:GetGroupQuery",
        "resource-groups:GetGroup"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationInsightsResourceGroup",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : [
        "arn:aws:resource-groups:*:*:group/ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "ElasticLoadBalancing",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
```

```
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AutoScaling",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:PutParameter",
        "ssm:DeleteParameter",
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource",
        "ssm:GetParameters"
      ],
      "Resource" : "arn:aws:ssm:*:*:parameter/AmazonCloudWatch-ApplicationInsights-*"
    },
    {
      "Sid" : "SSMAssociation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:CreateAssociation",
        "ssm:UpdateAssociation",
        "ssm:DeleteAssociation",
        "ssm:DescribeAssociation"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:association/*",
        "arn:aws:ssm:*:*:managed-instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-
ApplicationInsightsCloudwatchAgentInstallAndConfigure",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
```

```
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "SSMOpsItem",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsItem",
        "ssm:CreateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:UpdateOpsItem",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMTags",
      "Effect" : "Allow",
      "Action" : [
        "ssm:AddTagsToResource"
      ],
      "Resource" : "arn:aws:ssm:*:*:opsitem/*"
    },
    {
      "Sid" : "SSMGetCommandInvocation",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SSMSendCommand",
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ssm:*:*:document/AWSEC2-CheckPerformanceCounterSets",
        "arn:aws:ssm:*:*:document/AWS-ConfigureAWSPackage",
```

```
        "arn:aws:ssm:*:*:document/AWSEC2-DetectWorkload",
        "arn:aws:ssm:*:*:document/AmazonCloudWatch-ManageAgent"
      ]
    },
    {
      "Sid" : "EC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeNatGateways"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "RDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Lambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListFunctions",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EventBridgeManagedRule",
```

```
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/AmazonCloudWatch-ApplicationInsights-*"
      ]
    },
    {
      "Sid" : "XRay",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph",
        "xray:GetTraceSummaries",
        "xray:GetTimeSeriesServiceStatistics",
        "xray:GetTraceGraph"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscaling",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "S3",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets",
        "s3:GetMetricsConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "States",
      "Effect" : "Allow",
      "Action" : [
        "states:ListStateMachines",
        "states:DescribeExecution",
        "states:DescribeStateMachine",
        "states:GetExecutionHistory"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "APIGateway",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECS",
      "Effect" : "Allow",
      "Action" : [
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
```

```
        "ecs:DescribeServices",
        "ecs:DescribeTaskDefinition",
        "ecs:DescribeTasks",
        "ecs:DescribeTaskSets",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "ecs:ListTasks"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ECSCluster",
      "Effect" : "Allow",
      "Action" : [
        "ecs:UpdateClusterSettings"
      ],
      "Resource" : [
        "arn:aws:ecs:*:*:cluster/*"
      ]
    },
    {
      "Sid" : "EKS",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodegroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodegroups",
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SNS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sns:GetSubscriptionAttributes",
        "sns:GetTopicAttributes",
        "sns:GetSMSAttributes",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SQS",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ListQueues"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsDeleteSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid" : "CloudWatchLogsCreateSubscriptionFilter",
      "Effect" : "Allow",
      "Action" : [
        "logs:PutSubscriptionFilter"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:*",
        "arn:aws:logs:*:*:destination:AmazonCloudWatch-ApplicationInsights-
LogIngestionDestination*"
      ]
    },
    {
      "Sid" : "EFS",
      "Effect" : "Allow",
      "Action" : [
```

```
        "elasticfilesystem:DescribeFileSystems"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:GetHealthCheck",
        "route53:ListHostedZones",
        "route53:ListHealthChecks",
        "route53:ListQueryLoggingConfigs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Route53Resolver",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:ListResolverEndpoints",
        "route53resolver:GetResolverQueryLogConfig",
        "route53resolver:ListResolverQueryLogConfigs",
        "route53resolver:ListResolverQueryLogConfigAssociations",
        "route53resolver:GetResolverEndpoint",
        "route53resolver:GetFirewallRuleGroupAssociation"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsFullAccess

Beschreibung: Bieten Sie vollen Zugriff auf den CloudWatch Application Signals-Dienst und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für die Nutzung und den Betrieb dieses Dienstes erforderlich sind.

`CloudWatchApplicationSignalsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchApplicationSignalsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. Juni 2024, 22:50 UTC
- Bearbeitete Zeit: 20. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : "application-signals:*",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:DescribeAlarms",
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
```

```
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchCreateRumMetricDefinitions",
        "rum:BatchDeleteRumMetricDefinitions",
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "rum:PutRumMetricsDestination",
        "rum:UpdateRumMetricDefinition"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsPutMetricAlarmPermissions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricAlarm",
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:SLO-AttainmentGoalAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLO-WarningAlarm-*",
        "arn:aws:cloudwatch:*:*:alarm:SLI-HealthAlarm-*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCreateServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe"
      ],
      "Resource" : "arn:aws:sns:*:*:cloudwatch-application-signals-*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSnsReadPermissions",
      "Effect" : "Allow",
      "Action" : "sns:ListTopics",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
```

```
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf den CloudWatch Application Signals-Dienst und bereichsspezifischen Zugriff auf die Abhängigkeiten, die für die Nutzung dieses Dienstes erforderlich sind

`CloudWatchApplicationSignalsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchApplicationSignalsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 06. Juni 2024, 22:48 UTC
- Bearbeitete Zeit: 20. November 2025, 19:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchApplicationSignalsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
```

```
        "logs:StopQuery",
        "logs:GetQueryResults",
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsAlarmsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsMetricsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsSyntheticsReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:GetCanaryRuns"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsRumReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "rum:BatchGetRumMetricDefinitions",
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "CloudWatchApplicationSignalsXrayTracePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetTraceSummaries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsXrayReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:StartTraceRetrieval",
        "xray:ListRetrievedTraces",
        "xray:BatchGetTraces",
        "xray:GetTraceSegmentDestination"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "application-signals.cloudwatch.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "CloudWatchApplicationSignalsServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMAttachedLinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsOAMListSinksPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListSinks"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchApplicationSignalsServiceRolePolicy

Beschreibung: Die Richtlinie erteilt CloudWatch Application Signals die Erlaubnis, Überwachungs- und Kennzeichnungsdaten von anderen relevanten AWS Diensten zu sammeln.

`CloudWatchApplicationSignalsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2023, 18:09 UTC
- Bearbeitete Zeit: 14. November 2025, 21:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchApplicationSignalsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "XRayPermission",
      "Effect" : "Allow",
      "Action" : [
        "xray:GetServiceGraph"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWLogsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:StartQuery",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/appsignals/*:*",
        "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "CWListMetricsPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CWGetMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "TagsPermission",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "ApplicationSignalsPermission",
      "Effect" : "Allow",
      "Action" : [
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:GetServiceLevelObjective"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2AutoScalingPermission",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceExplorerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudTrailServiceLinkedChannelCreationPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudtrail:CreateServiceLinkedChannel"
      ],
      "Resource" : [
        "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-signals/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchAutomaticDashboardsAccess

Beschreibung: Bietet Zugriff auf CloudWatch automatische Dashboards, die nicht zur Anzeige CloudWatch APIs verwendet werden, einschließlich des Inhalts von Objekten wie Lambda-Funktionen

`CloudWatchAutomaticDashboardsAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchAutomaticDashboardsAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Juli 2019, 10:01 UTC
- Bearbeitete Zeit: 20. April 2021, 13:05 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchAutomaticDashboardsAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:DescribeClusters",
        "ecs:DescribeContainerInstances",
        "ecs:ListClusters",
        "ecs:ListContainerInstances",
        "ecs:ListServices",
        "elasticache:DescribeCacheClusters",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeLoadBalancers",
        "kinesis:DescribeStream",
        "kinesis:ListStreams",
        "lambda:GetFunction",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "resource-groups:ListGroupResources",
        "resource-groups:ListGroups",
        "route53:GetHealthCheck",
        "route53:ListHealthChecks",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
```

```
        "sqs:ListQueues",
        "synthetics:DescribeCanariesLastRun",
        "tag:GetResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "apigateway:GET"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:apigateway:*::/restapis*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur Einrichtung der gemeinsamen Nutzung von CloudWatch Ressourcen

`CloudWatchCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 14:01 UTC
- Bearbeitete Zeit: 27. November 2022, 14:01 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsBuiltInTargetExecutionAccess

Beschreibung: Ermöglicht integrierten Zielen in Amazon CloudWatch Events, EC2 Aktionen in Ihrem Namen durchzuführen.

`CloudWatchEventsBuiltInTargetExecutionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchEventsBuiltInTargetExecutionAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2016, 18:35 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:35 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsBuiltInTargetExecutionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsBuiltInTargetExecutionAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:Describe*",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon CloudWatch Events.

`CloudWatchEventsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchEventsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2016, 18:37 UTC
- Bearbeitete Zeit: 22. Januar 2025, 02:07 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsFullAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EventBridgeActions",
      "Effect" : "Allow",
      "Action" : [
        "events:*",
        "schemas:*",
        "scheduler:*",
        "pipes:*"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForApiDestinations",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "apidestinations.events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMCreateServiceLinkedRoleForAmazonEventBridgeSchemas",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/schemas.amazonaws.com/
AWSServiceRoleForSchemas",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "schemas.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SecretsManagerAccessForApiDestinations",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:events!*"
    },
    {
      "Sid" : "IAMPassRoleForCloudWatchEvents",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/AWS_Events_Invoke_Targets"
```

```
    },
    {
      "Sid" : "IAMPassRoleAccessForScheduler",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "scheduler.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMPassRoleAccessForPipes",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "pipes.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsInvocationAccess

Beschreibung: Ermöglicht Amazon CloudWatch Events, Ereignisse an die Streams in AWS Kinesis Streams in Ihrem Konto weiterzuleiten.

`CloudWatchEventsInvocationAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchEventsInvocationAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Januar 2016, 18:36 Uhr UTC
- Bearbeitete Zeit: 14. Januar 2016, 18:36 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/CloudWatchEventsInvocationAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchEventsInvocationAccess",
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon CloudWatch Events.

`CloudWatchEventsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchEventsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 14. Januar 2016, 18:27 UTC
- Bearbeitete Zeit: 1. Dezember 2022, 16:29 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchEventsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "events:DescribeRule",
        "events:DescribeEventBus",
        "events:DescribeEventSource",
        "events:ListEventBuses",
        "events:ListEventSources",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "events:TestEventPattern",
        "events:DescribeArchive",
        "events:ListArchives",
        "events:DescribeReplay",
        "events:ListReplays",
        "events:DescribeConnection",
        "events:ListConnections",
        "events:DescribeApiDestination",
        "events:ListApiDestinations",
        "events:DescribeEndpoint",
        "events:ListEndpoints",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:ExportSchema",
        "schemas:GetCodeBindingSource",
        "schemas:GetDiscoveredSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "schemas:SearchSchemas",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListSchedules",
        "scheduler:ListScheduleGroups",
        "scheduler:ListTagsForResource",
        "pipes:DescribePipe",
```

```
        "pipes:ListPipes",
        "pipes:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchEventsServiceRolePolicy

Beschreibung: Ermöglicht AWS CloudWatch die Ausführung von Aktionen in Ihrem Namen, die über Alarme und Ereignisse konfiguriert wurden.

`CloudWatchEventsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. November 2017, 00:42 UTC
- Zeit bearbeitet: 17. November 2017, 00:42 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchEventsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RebootInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch.

`CloudWatchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Zeit bearbeitet: 27. November 2022, 13:23 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudwatch:*",
        "logs:*",
        "sns:*",
        "iam:GetPolicy",
```

```
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchFullAccessV2

Beschreibung: Bietet vollen Zugriff auf CloudWatch.

`CloudWatchFullAccessV2`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchFullAccessV2` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. August 2023, 11:32 UTC
- Bearbeitete Zeit: 2. Dezember 2025, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchFullAccessV2`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchFullAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "cloudwatch:*",
        "logs:*",
        "sns:CreateTopic",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics",
        "sns:Subscribe",
```

```
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:GetRole",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:CreateCentralizationRuleForOrganization",
        "observabilityadmin:UpdateCentralizationRuleForOrganization",
        "observabilityadmin:DeleteCentralizationRuleForOrganization",
        "observabilityadmin:StartTelemetryEvaluation",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:StopTelemetryEvaluation",
        "observabilityadmin:StartTelemetryEvaluationForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:StopTelemetryEvaluationForOrganization",
        "observabilityadmin:CreateTelemetryRule",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:UpdateTelemetryRule",
        "observabilityadmin:DeleteTelemetryRule",
        "observabilityadmin:CreateTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:UpdateTelemetryRuleForOrganization",
        "observabilityadmin:DeleteTelemetryRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:StartTelemetryEnrichment",
        "observabilityadmin:StopTelemetryEnrichment",
        "observabilityadmin:TagResource",
        "observabilityadmin:UntagResource",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:CreateTelemetryPipeline",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:UpdateTelemetryPipeline",
        "observabilityadmin:DeleteTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:CreateS3TableIntegration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:DeleteS3TableIntegration",
```

```
        "rum:*",
        "synthetics:*",
        "xray:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsServiceLinkedRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "application-signals.cloudwatch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EventsServicePermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/events.amazonaws.com/
AWSServiceRoleForCloudWatchEvents*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "events.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:GetChannel"
```

```
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchApplicationSignalsCloudTrailListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:ListChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchResourceExplorerSLRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/resource-
explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "resource-explorer-2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchResourceExplorerCreateIndexPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:CreateIndex"
      ],
      "Resource" : "arn:aws:resource-explorer-2:*:*:index/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "logs.amazonaws.com"
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" :
 "arn:aws:observabilityadmin:*:*:s3tableintegration/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "iam:PassedToService" : [
            "logs.amazonaws.com",
            "telemetry-pipelines.observabilityadmin.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:observabilityadmin:*:*:telemetry-
pipeline/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:CreateTableBucket",
        "s3tables:PutTableBucketEncryption"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "observabilityadmin.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3tables:PutTableBucketPolicy"
      ],
      "Resource" : "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchInternetMonitorFullAccess

Beschreibung: Bietet vollen Zugriff auf Aktionen für die Arbeit mit Amazon CloudWatch Internet Monitor. Bietet auch Zugriff auf andere Dienste wie Amazon, Amazon CloudWatch EC2, Amazon CloudFront und Elastic Load Balancing WorkSpaces, die für die Nutzung des Internet Monitor-Dienstes zur Überwachung und Speicherung von Informationen über den Anwendungsverkehr erforderlich sind.

`CloudWatchInternetMonitorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchInternetMonitorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Oktober 2024, 21:02 UTC
- Bearbeitete Zeit: 22. Oktober 2024, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "FullAccessActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "internetmonitor:CreateMonitor",
        "internetmonitor:DeleteMonitor",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:Link",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "internetmonitor:TagResource",
        "internetmonitor:UntagResource",
        "internetmonitor:UpdateMonitor"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ServiceLinkedRoleActions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "internetmonitor.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "RolePolicyActions",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/internetmonitor.amazonaws.com/
AWSServiceRoleForInternetMonitor",
      "Condition" : {
        "ArnEquals" : {
```

```
          "iam:PolicyARN" : "arn:aws:iam::aws:policy/aws-service-role/
CloudWatchInternetMonitorServiceRolePolicy"
        }
      }
    },
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudfront:GetDistribution",
        "cloudfront:ListDistributions",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchInternetMonitorReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Aktionen für die Arbeit mit Amazon CloudWatch Internet Monitor. Bietet auch Zugriff auf andere Dienste von Amazon CloudWatch, einschließlich Richtlinien zum Abrufen von Informationen zu CloudWatch Messwerten und zur Verwaltung von Protokollabfragen, die für die Nutzung des Internet Monitor-Dienstes zur Überwachung und Speicherung von Informationen über den Anwendungsverkehr erforderlich sind.

`CloudWatchInternetMonitorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchInternetMonitorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2024, 23:11 UTC
- Bearbeitete Zeit: 12. November 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchInternetMonitorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:GetQueryResults",
        "internetmonitor:GetQueryStatus",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
```

```
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "internetmonitor:StartQuery",
        "internetmonitor:StopQuery",
        "logs:DescribeLogGroups",
        "logs:GetQueryResults",
        "logs:StartQuery",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchInternetMonitorServiceRolePolicy

Beschreibung: Ermöglicht Internet Monitor den Zugriff auf EC2 Arbeitsbereiche und CloudFront Ressourcen sowie andere erforderliche Dienste in Ihrem Namen.

`CloudWatchInternetMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 27. November 2022, 17:46 UTC

- Bearbeitete Zeit: 20. Juli 2023, 04:46 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchInternetMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
      ],
```

```
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/internet-monitor/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/InternetMonitor"
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLambdaApplicationSignalsExecutionRolePolicy

Beschreibung: Ermöglicht Schreibzugriff auf die Protokollgruppe X-Ray und CloudWatch Application Signals.

`CloudWatchLambdaApplicationSignalsExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchLambdaApplicationSignalsExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. Oktober 2024, 19:09 UTC
- Bearbeitete Zeit: 16. Oktober 2024, 19:09 UTC

- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaApplicationSignalsExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchApplicationSignalsXrayWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "xray:PutTraceSegments"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CloudWatchApplicationSignalsLogGroupWritePermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/application-signals/data:*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLambdaInsightsExecutionRolePolicy

Beschreibung: Für die Lambda Insights-Erweiterung ist eine Richtlinie erforderlich

`CloudWatchLambdaInsightsExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchLambdaInsightsExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. Oktober 2020, 19:27 UTC
- Zeit bearbeitet: 7. Oktober 2020, 19:27 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda-insights:*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsCrossAccountSharingConfiguration

Beschreibung: Bietet Funktionen zur Verwaltung von Observability Access Manager-Links und zur gemeinsamen Nutzung von CloudWatch Logs-Ressourcen

`CloudWatchLogsCrossAccountSharingConfiguration`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchLogsCrossAccountSharingConfiguration` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:55 UTC
- Zeit bearbeitet: 27. November 2022, 13:55 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsCrossAccountSharingConfiguration`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:Link",
        "oam:ListLinks"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "oam:DeleteLink",
        "oam:GetLink",
        "oam:TagResource"
      ],
      "Resource" : "arn:aws:oam:*:*:link/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:CreateLink",
        "oam:UpdateLink"
      ],
      "Resource" : [
        "arn:aws:oam:*:*:link/*",
        "arn:aws:oam:*:*:sink/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Protokolle

`CloudWatchLogsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchLogsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 2. Dezember 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchLogsReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Protokolle

`CloudWatchLogsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchLogsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 2. Dezember 2025, 16:34 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchLogsReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:Describe*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListTelemetryPipelines"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkFlowMonitorAgentPublishPolicy

Beschreibung: Sie können diese Richtlinie in IAM-Rollen verwenden, die Amazon EC2 - und Amazon EKS-Instance-Ressourcen zugeordnet sind, um Telemetrieberichte (Metriken) an einen Network Flow Monitor-Endpunkt zu senden.

`CloudWatchNetworkFlowMonitorAgentPublishPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchNetworkFlowMonitorAgentPublishPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2024, 22:51 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 22:51 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchNetworkFlowMonitorAgentPublishPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "networkflowmonitor:Publish"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkFlowMonitorServiceRolePolicy

Beschreibung: Sie können keine Verbindungen CloudWatchNetworkFlowMonitorServiceRolePolicy zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist einer dienstbezogenen Rolle mit dem Namen zugeordnet AWSServiceRoleForNetworkFlowMonitor, die die von Network Flow Monitor-Agenten gesammelten Ergebnisse der Netzwerktelemetrie-Aggregation veröffentlicht. CloudWatch Es ermöglicht dem Dienst auch, AWS Organizations zu verwenden, um Informationen für Szenarien mit mehreren Konten abzurufen.

`CloudWatchNetworkFlowMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2024, 22:36 UTC
- Bearbeitete Zeit: 29. April 2025, 10:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkFlowMonitor"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/*"
      ]
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy

Beschreibung: Sie können keine Verbindungen CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy zu Ihren IAM-Entitäten herstellen. Diese Richtlinie ist einer dienstbezogenen Rolle mit dem Namen zugeordnet AWSServiceRoleForNetworkFlowMonitor_Topology, die Topologie-Snapshots der Ressourcen generiert, die von Network Flow Monitor in Ihrem Konto verwendet werden.

`CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 1. Dezember 2024, 22:51 UTC
- Bearbeitete Zeit: 10. Dezember 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkFlowMonitorTopologyServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayConnects",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeCustomerGateways",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrefixListStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeManagedPrefixLists",
        "ec2:GetManagedPrefixListEntries"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "VPCEndpointStatement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchNetworkMonitorServiceRolePolicy

Beschreibung: Ermöglicht CloudWatch Network Monitor den Zugriff auf und die Verwaltung von EC2 VPC-Ressourcen, die Veröffentlichung von Daten CloudWatch und den Zugriff auf andere erforderliche Dienste in Ihrem Namen.

`CloudWatchNetworkMonitorServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Dezember 2023, 18:53 UTC
- Bearbeitete Zeit: 12. Dezember 2025, 22:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CloudWatchNetworkMonitorServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PublishCw",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NetworkMonitor"
        }
      }
    },
    {
      "Sid" : "DescribeAny",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteModifyEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
```

```
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/ManagedByCloudWatchNetworkMonitor" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchOpenSearchDashboardAccess

Beschreibung: Diese Richtlinie bietet Benutzern Zugriff auf die Anzeige von OpenSearch Dashboards in der CloudWatch Logs-Konsole.

`CloudWatchOpenSearchDashboardAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchOpenSearchDashboardAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 1. Dezember 2024, 21:06 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
```

```
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDirectQueryStatusAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchOpenSearchDashboardsFullAccess

Beschreibung: Diese Richtlinie bietet Benutzern Zugriff auf Create Integration OpenSearch zum Erstellen, Aktualisieren, Löschen oder Anzeigen von Dashboards in der CloudWatch Logs-Konsole.

`CloudWatchOpenSearchDashboardsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchOpenSearchDashboardsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2024, 21:06 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 21:06 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchOpenSearchDashboardsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchOpenSearchDashboardsIntegration",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListIntegrations",
        "logs:GetIntegration",
        "logs:DeleteIntegration",
```

```
        "logs:PutIntegration",
        "logs:DescribeLogGroups",
        "opensearch:ApplicationAccessAll",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsOpensearchReadAPIs",
      "Effect" : "Allow",
      "Action" : [
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "es:ListApplications"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsOpensearchCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsObservabilityCreateServiceLinkedAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationRequestAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:CreateApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
```

```
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:DeleteCollection"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsApplicationResourceAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:UpdateApplication",
        "es:GetApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsCollectionPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateSecurityPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:DeleteSecurityPolicy",
```

```
        "aoss:GetAccessPolicy",
        "aoss:GetSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAPIAccessAll",
      "Effect" : "Allow",
      "Action" : [
        "aoss:APIAccessAll"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "cloudwatch-logs-*"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsIndexPolicyAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:CreateLifecyclePolicy",
        "aoss:DeleteLifecyclePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aoss:index" : "cloudwatch-logs-*",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsDQSRequestQueryAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "es:AddDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:RequestTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsStartDirectQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "opensearch:StartDirectQuery",
        "opensearch:GetDirectQuery"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*"
    },
    {
      "Sid" : "CloudWatchLogsDQSResourceQueryAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:GetDirectQueryDataSource",
        "es:DeleteDirectQueryDataSource"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/cloudwatch_logs_*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        }
      }
    },
    {
```

```
      "Sid" : "CloudWatchLogsPassRoleAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "directquery.opensearchservice.amazonaws.com",
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsAossTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "aoss:TagResource"
      ],
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "logs.amazonaws.com",
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ]
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsApplicationTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:application/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/OpenSearchIntegration" : [
            "Dashboards"
          ],
```

```
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "OpenSearchIntegration"
        }
      }
    },
    {
      "Sid" : "CloudWatchLogsEsDataSourceTagsAccess",
      "Effect" : "Allow",
      "Action" : [
        "es:AddTags"
      ],
      "Resource" : "arn:aws:opensearch:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CloudWatchOpenSearchIntegration" : [
            "Dashboards"
          ],
          "aws:CalledViaFirst" : "logs.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "CloudWatchOpenSearchIntegration"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch.

`CloudWatchReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 2. Dezember 2025, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v14 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CloudWatchReadOnlyAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalingPolicies",
        "application-signals:BatchGet*",
        "application-signals:Get*",
        "application-signals:List*",
        "autoscaling:Describe*",
        "cloudtrail:ListChannels",
        "cloudwatch:BatchGet*",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
```

```
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:List*",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "logs:FilterLogEvents",
        "logs:StartLiveTail",
        "logs:StopLiveTail",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:GetS3TableIntegration",
        "observabilityadmin:ListS3TableIntegrations",
        "sns:Get*",
        "sns:List*",
        "rum:BatchGet*",
        "rum:Get*",
        "rum:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "xray:BatchGet*",
        "xray:Get*",
        "xray:List*",
        "xray:StartTraceRetrieval",
        "xray:CancelTraceRetrieval"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "OAMReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "oam:ListAttachedLinks"
      ],
      "Resource" : "arn:aws:oam:*:*:sink/*"
    },
    {
      "Sid" : "CloudWatchReadOnlyGetRolePermissions",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/application-
signals.cloudwatch.amazonaws.com/AWSServiceRoleForCloudWatchApplicationSignals"
    },
    {
      "Sid" : "CloudWatchCloudTrailPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:GetChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/application-
signals/*"
    },
    {
      "Sid" : "CloudWatchServiceQuotaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : [
        "arn:aws:servicequotas:*:*:s3/*",
        "arn:aws:servicequotas:*:*:dynamodb/*",
        "arn:aws:servicequotas:*:*:kinesis/*",
        "arn:aws:servicequotas:*:*:sns/*",
        "arn:aws:servicequotas:*:*:bedrock/*",
        "arn:aws:servicequotas:*:*:lambda/*",
        "arn:aws:servicequotas:*:*:fargate/*",
        "arn:aws:servicequotas:*:*:elasticloadbalancing/*",
        "arn:aws:servicequotas:*:*:ec2/*"
      ]
    },
```

```
    {
      "Sid" : "CloudWatchResourceExplorerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:Search"
      ],
      "Resource" : [
        "arn:aws:resource-explorer-2:*::view/AWSServiceViewForApplicationSignals/
service-view",
        "arn:aws:resource-explorer-2:*::view/
AWSServiceViewForApplicationSignalsOrgScopeProd/service-view"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchSyntheticsFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Synthetics.

`CloudWatchSyntheticsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchSyntheticsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. November 2019, 17:39 Uhr UTC

- Bearbeitete Zeit: 21. November 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsFullAccess`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::cw-syn-results-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "s3:ListAllMyBuckets",
        "xray:GetTraceSummaries",
        "xray:BatchGetTraces",
```

```
        "apigateway:GET"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::cw-syn-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::aws-synthetics-library-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com",
            "synthetics.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : [
        "arn:aws:cloudwatch:*:*:alarm:*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:GetLogRecord",
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:FilterLogEvents",
```

```
        "logs:GetLogGroupFields"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/cwsyn-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "lambda:PublishVersion",
        "lambda:UpdateFunctionCode",
        "lambda:UpdateFunctionConfiguration",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunction",
        "lambda:DeleteFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:cwsyn-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetLayerVersion",
        "lambda:PublishLayerVersion",
        "lambda:DeleteLayerVersion"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:layer:cwsyn-*",
        "arn:aws:lambda:*:*:layer:Synthetics:*",
        "arn:aws:lambda:*:*:layer:Synthetics_Selenium:*",
        "arn:aws:lambda:*:*:layer:AWS-CW-Synthetics*:*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : [
        "arn:*:sns:*:*:Synthetics-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*"
```

```
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CloudWatchSyntheticsReadOnlyAccess

Beschreibung: Bietet Nur-Lese-Zugriff auf CloudWatch Synthetics.

`CloudWatchSyntheticsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CloudWatchSyntheticsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 25. November 2019, 17:45 Uhr UTC
- Bearbeitete Zeit: 6. März 2020, 19:26 UTC
- ARN: `arn:aws:iam::aws:policy/CloudWatchSyntheticsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendDataAccessRolePolicy

Beschreibung: Richtlinie für die AWS Servicerolle Comprehend, die den Zugriff auf S3-Ressourcen für den Datenzugriff ermöglicht

`ComprehendDataAccessRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ComprehendDataAccessRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 06. März 2019, 22:28 Uhr UTC
- Bearbeitete Zeit: 6. März 2019, 22:28 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ComprehendDataAccessRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : {
    "Effect" : "Allow",
    "Action" : [
      "s3:GetObject",
      "s3:ListBucket",
      "s3:PutObject"
    ],
    "Resource" : [
```

```
      "arn:aws:s3:::*Comprehend*",
      "arn:aws:s3:::*comprehend*"
    ]
  }
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Comprehend.

`ComprehendFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ComprehendFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:08 Uhr UTC
- Bearbeitete Zeit: 5. Dezember 2017, 01:36 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehend:*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendMedicalFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Comprehend Medical

`ComprehendMedicalFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ComprehendMedicalFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 17:55 Uhr UTC
- Bearbeitete Zeit: 27. November 2018, 17:55 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendMedicalFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "comprehendmedical:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComprehendReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Comprehend.

`ComprehendReadOnly`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `ComprehendReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:10 Uhr UTC
- Bearbeitete Zeit: 26. April 2022, 21:32 UTC
- ARN: `arn:aws:iam::aws:policy/ComprehendReadOnly`

Version der Richtlinie

Richtlinienversion: v11 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectDominantLanguage",
        "comprehend:BatchDetectDominantLanguage",
        "comprehend:DetectEntities",
        "comprehend:BatchDetectEntities",
        "comprehend:DetectKeyPhrases",
        "comprehend:BatchDetectKeyPhrases",
```

```
        "comprehend:DetectPiiEntities",
        "comprehend:ContainsPiiEntities",
        "comprehend:DetectSentiment",
        "comprehend:BatchDetectSentiment",
        "comprehend:DetectSyntax",
        "comprehend:BatchDetectSyntax",
        "comprehend:ClassifyDocument",
        "comprehend:DescribeTopicsDetectionJob",
        "comprehend:ListTopicsDetectionJobs",
        "comprehend:DescribeDominantLanguageDetectionJob",
        "comprehend:ListDominantLanguageDetectionJobs",
        "comprehend:DescribeEntitiesDetectionJob",
        "comprehend:ListEntitiesDetectionJobs",
        "comprehend:DescribeKeyPhrasesDetectionJob",
        "comprehend:ListKeyPhrasesDetectionJobs",
        "comprehend:DescribePiiEntitiesDetectionJob",
        "comprehend:ListPiiEntitiesDetectionJobs",
        "comprehend:DescribeSentimentDetectionJob",
        "comprehend:DescribeTargetedSentimentDetectionJob",
        "comprehend:ListSentimentDetectionJobs",
        "comprehend:ListTargetedSentimentDetectionJobs",
        "comprehend:DescribeDocumentClassifier",
        "comprehend:ListDocumentClassifiers",
        "comprehend:DescribeDocumentClassificationJob",
        "comprehend:ListDocumentClassificationJobs",
        "comprehend:DescribeEntityRecognizer",
        "comprehend:ListEntityRecognizers",
        "comprehend:ListTagsForResource",
        "comprehend:DescribeEndpoint",
        "comprehend:ListEndpoints",
        "comprehend:ListDocumentClassifierSummaries",
        "comprehend:ListEntityRecognizerSummaries",
        "comprehend:DescribeResourcePolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComputeOptimizerAutomationServiceRolePolicy

Beschreibung: Die ComputeOptimizerAutomationServiceRolePolicy verwaltete Richtlinie ist an eine serviceverknüpfte Rolle angehängt, die es Compute Optimizer ermöglicht, Aktionen in Ihrem Namen durchzuführen

`ComputeOptimizerAutomationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2025, 01:19 UTC
- Zeit bearbeitet: 15. November 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerAutomationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EBSReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EBSVolumeModification",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVolume",
        "ec2:DeleteVolume"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/exclude-from-compute-optimizer-automation" : "true"
        }
      }
    },
    {
      "Sid" : "CreateEBSSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RollbackEBSVolumeDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Tag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComputeOptimizerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf ComputeOptimizer.

`ComputeOptimizerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ComputeOptimizerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 7. März 2020, 00:11 UTC
- Bearbeitete Zeit: 20. November 2024, 21:08 UTC
- ARN: `arn:aws:iam::aws:policy/ComputeOptimizerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "computeOptimizerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetRecommendationSummaries",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
```

```
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetIdleRecommendations",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ecs:ListServices",
        "ecs:ListClusters",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "lambda:ListFunctions",
        "lambda:ListProvisionedConcurrencyConfigs",
        "cloudwatch:GetMetricData",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ComputeOptimizerServiceRolePolicy

Beschreibung: Ermöglicht ComputeOptimizer das Aufrufen von AWS Diensten und das Sammeln von Workload-Details in Ihrem Namen.

`ComputeOptimizerServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 3. Dezember 2019, 08:45 Uhr UTC
- Bearbeitete Zeit: 19. November 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ComputeOptimizerServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ComputeOptimizerFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "compute-optimizer:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
```

```
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CloudWatchAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AutoScalingAccess",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribePolicies",
        "autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ec2Access",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ConfigConformsServiceRolePolicy

Beschreibung: Richtlinie, die für AWSConfig die Erstellung von Konformitätspaketen erforderlich ist

`ConfigConformsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Juli 2019, 21:38 Uhr UTC
- Bearbeitete Zeit: 12. Januar 2023, 04:17 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ConfigConformsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "config:PutConfigRule",
        "config:DeleteConfigRule"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/config-
conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigRules"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeRemediationConfigurations",
        "config:DeleteRemediationConfiguration",
        "config:PutRemediationConfigurations"
      ],
      "Resource" : "arn:aws:config:*:*:remediation-configuration/aws-service-
remediation-configuration/config-conforms.amazonaws.com*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/config-conforms.amazonaws.com/
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
```

```
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
remediation.config.amazonaws.com/AWSServiceRoleForConfigRemediation",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "remediation.config.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ssm.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetBucketAcl"
      ],
      "Resource" : "arn:aws:s3:::awsconfigconforms*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStacks",
        "cloudformation:GetStackPolicy",
        "cloudformation:SetStackPolicy",
        "cloudformation:UpdateStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:ValidateTemplate",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/awsconfigconforms-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Config"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ConsoleFullAccessFromVercel

Beschreibung: Zur Verwendung mit Konten, die über die Vercel Marketplace-Integration mit AWS erstellt wurden. Bietet Zugriff auf die Verwaltung aller Ressourcen für die Dienste, die in den Vercel Marketplace integriert sind.

`ConsoleFullAccessFromVercel`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ConsoleFullAccessFromVercel` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2025, 16:49 UTC
- Bearbeitete Zeit: 11. Dezember 2025, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleFullAccessFromVercel`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
```

```
        "dsql:UpdateCluster",
        "dsql:DbConnectAdmin",
        "dsql:DbConnect"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:ConditionCheckItem",
        "dynamodb:UntagResource",
        "dynamodb:PutItem",
        "dynamodb:ListTables",
        "dynamodb:DeleteItem",
        "dynamodb:Scan",
        "dynamodb:ListTagsOfResource",
        "dynamodb:Query",
        "dynamodb:UpdateItem",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:TagResource",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:DescribeLimits",
        "dynamodb:UpdateTable",
        "dynamodb:GetRecords"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds-db:connect",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rds:RebootDBInstance",
```

```
        "rds:DeleteDBInstance",
        "rds:StartDBInstance",
        "rds:ModifyDBInstance",
        "rds:ApplyPendingMaintenanceAction",
        "rds:StartDBCluster",
        "rds:DeleteDBCluster",
        "rds:RebootDBCluster",
        "rds:CreateDBClusterEndpoint",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:FailoverDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:ModifyDBClusterParameterGroup",
        "rds:CopyDBClusterParameterGroup",
        "rds:ResetDBClusterParameterGroup",
        "rds:CreateDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:ModifyDBParameterGroup",
        "rds:CopyDBParameterGroup",
        "rds:DeleteDBParameterGroup",
        "rds:CreateDBParameterGroup",
        "rds:DeleteDBClusterAutomatedBackup",
        "rds:CopyDBClusterSnapshot",
        "rds:RestoreDBClusterToPointInTime",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:DeleteDBClusterSnapshot",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AuroraRestricted",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "rds:DatabaseEngine" : "aurora-postgresql"
        }
      }
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "cloudwatch:PutMetricAlarm",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingIntegration",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : "dynamodb"
        }
      }
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ViewFreeTierState",
      "Effect" : "Allow",
      "Action" : [
        "freetier:GetAccountPlanState"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ConsoleViewOnlyAccessFromVercel

Beschreibung: Zur Verwendung mit Konten, die über die Vercel Marketplace-Integration mit AWS erstellt wurden. Bietet Zugriff auf alle Ressourcen für die Dienste, die in den Vercel Marketplace integriert sind.

`ConsoleViewOnlyAccessFromVercel`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ConsoleViewOnlyAccessFromVercel` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2025, 16:49 UTC
- Bearbeitete Zeit: 11. Dezember 2025, 16:49 UTC
- ARN: `arn:aws:iam::aws:policy/ConsoleViewOnlyAccessFromVercel`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DSQL",
      "Effect" : "Allow",
      "Action" : [
        "dsql:GetCluster",
        "dsql:ListClusters",
        "dsql:ListTagsForResource"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DynamoDB",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:DescribeTimeToLive",
```

```
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Aurora",
      "Effect" : "Allow",
      "Action" : [
        "rds:Describe*",
        "rds:ListTagsForResource",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Observability",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "tag:GetTagKeys",
        "tag:GetTagValues"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ApplicationAutoscalingDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubAdminAccess

Beschreibung: Diese verwaltete Richtlinie bietet Administratorzugriff auf Cost Optimization Hub.

`CostOptimizationHubAdminAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CostOptimizationHubAdminAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Dezember 2023, 00:03 Uhr UTC
- Zeit bearbeitet: 19. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubAdminAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubAdminAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:UpdateEnrollmentStatus",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:UpdatePreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowCreationOfServiceLinkedRoleForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/cost-optimization-hub.bcm.amazonaws.com/
AWSServiceRoleForCostOptimizationHub"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "cost-optimization-hub.bcm.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowAWSServiceAccessForCostOptimizationHub",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubReadOnlyAccess

Beschreibung: Diese verwaltete Richtlinie bietet schreibgeschützten Zugriff auf Cost Optimization Hub.

`CostOptimizationHubReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `CostOptimizationHubReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Dezember 2023, 18:04 UTC
- Bearbeitete Zeit: 19. November 2025, 16:49 UTC

- ARN: `arn:aws:iam::aws:policy/CostOptimizationHubReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CostOptimizationHubReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListEfficiencyMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CostOptimizationHubServiceRolePolicy

Beschreibung: Ermöglicht Cost Optimization Hub, Unternehmensinformationen abzurufen und optimierungsbezogene Daten und Metadaten zu sammeln.

`CostOptimizationHubServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2023, 08:03 UTC
- Bearbeitete Zeit: 17. Juli 2025, 18:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CostOptimizationHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AwsOrgsScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "cost-optimization-hub.bcm.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CostExplorerAccess",
      "Effect" : "Allow",
      "Action" : [
        "ce:ListCostAllocationTags",
        "ce:GetCostAndUsage",
        "ce:GetDimensionValues"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

CustomerProfilesServiceLinkedRolePolicy

Beschreibung: Ermöglicht Amazon Connect Connect-Kundenprofilen den Zugriff auf AWS Dienste und Ressourcen in Ihrem Namen.

`CustomerProfilesServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. März 2023, 22:56 UTC
- Bearbeitete Zeit: 26. November 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/CustomerProfilesServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/CustomerProfiles"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/profile.amazonaws.com/
AWSServiceRoleForProfile_*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "connect-campaigns:PutProfileOutboundRequestBatch"
      ],
      "Resource" : [
        "arn:aws:connect-campaigns:*:*:campaign/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "profile:BatchGetProfile"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DatabaseAdministrator

Beschreibung: Gewährt volle Zugriffsberechtigungen für AWS Dienste und Aktionen, die für die Einrichtung und Konfiguration von AWS Datenbankdiensten erforderlich sind.

`DatabaseAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `DatabaseAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:25 Uhr UTC
- Zeit bearbeitet: 1. Oktober 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DatabaseAdministrator`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms",
```

```
        "cloudwatch:Describe*",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:EnableAlarmActions",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudwatch:PutMetricAlarm",
        "datapipeline:ActivatePipeline",
        "datapipeline:CreatePipeline",
        "datapipeline:DeletePipeline",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:PutPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticache:*",
        "iam:ListRoles",
        "iam:GetRole",
        "kms:ListKeys",
        "lambda:CreateEventSourceMapping",
        "lambda:CreateFunction",
        "lambda:DeleteEventSourceMapping",
        "lambda:DeleteFunction",
        "lambda:GetFunctionConfiguration",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:Create*",
        "logs:PutLogEvents",
        "logs:PutMetricFilter",
        "pi:CreatePerformanceAnalysisReport",
        "pi:DeletePerformanceAnalysisReport",
        "pi:DescribeDimensionKeys",
```

```
        "pi:GetDimensionKeyDetails",
        "pi:GetPerformanceAnalysisReport",
        "pi:GetResourceMetadata",
        "pi:GetResourceMetrics",
        "pi:ListAvailableResourceDimensions",
        "pi:ListAvailableResourceMetrics",
        "pi:ListPerformanceAnalysisReports",
        "pi:ListTagsForResource",
        "pi:TagResource",
        "pi:UntagResource",
        "rds:*",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:DeleteTopic",
        "sns:Get*",
        "sns:List*",
        "sns:SetTopicAttributes",
        "sns:Subscribe",
        "sns:Unsubscribe"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutBucketWebsite",
        "s3:PutLifecycleConfiguration",
        "s3:PutReplicationConfiguration",
        "s3:PutObject*",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/rdbms-lambda-access",
        "arn:aws:iam::*:role/lambda_exec_role",
        "arn:aws:iam::*:role/lambda-dynamodb-*",
        "arn:aws:iam::*:role/lambda-vpc-execution-role",
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DataScientist

Beschreibung: Erteilt Berechtigungen für AWS Datenanalysedienste.

`DataScientistist` eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `DataScientist` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:28 Uhr UTC

- Bearbeitete Zeit: 3. Dezember 2019, 16:48 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/DataScientist`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "autoscaling:*",
        "cloudwatch:*",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackEvents",
        "datapipeline:Describe*",
        "datapipeline:ListPipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:QueryObjects",
        "dynamodb:*",
        "ec2:CancelSpotInstanceRequests",
        "ec2:CancelSpotFleetRequests",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "ec2:ModifyImageAttribute",
        "ec2:ModifyInstanceAttribute",
        "ec2:ModifySpotFleetRequest",
        "ec2:RequestSpotInstances",
        "ec2:RequestSpotFleet",
        "elasticfilesystem:*",
        "elasticmapreduce:*",
        "es:*",
```

```
        "firehose:*",
        "fsx:DescribeFileSystems",
        "iam:GetInstanceProfile",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:ListRoles",
        "kinesis:*",
        "kms:List*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:PublishVersion",
        "lambda:Update*",
        "lambda:List*",
        "machinelearning:*",
        "sdb:*",
        "rds:*",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "redshift:*",
        "s3:CreateBucket",
        "sns:CreateTopic",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:Abort*",
        "s3:DeleteObject",
        "s3:Get*",
        "s3:List*",
        "s3:PutAccelerateConfiguration",
        "s3:PutBucketCors",
        "s3:PutBucketLogging",
        "s3:PutBucketNotification",
        "s3:PutBucketTagging",
```

```
        "s3:PutObject",
        "s3:Replicate*",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/DataPipelineDefaultRole",
        "arn:aws:iam::*:role/DataPipelineDefaultResourceRole",
        "arn:aws:iam::*:role/EMR_EC2_DefaultRole",
        "arn:aws:iam::*:role/EMR_DefaultRole",
        "arn:aws:iam::*:role/kinesis-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "sagemaker.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*"
      ],
      "NotResource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*",
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:flow-definition/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:DescribeDomain",
        "sagemaker:ListDomains",
        "sagemaker:DescribeUserProfile",
        "sagemaker:ListUserProfiles",
        "sagemaker:*App",
        "sagemaker:ListApps"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:*FlowDefinition",
        "sagemaker:*FlowDefinitions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "sagemaker:WorkteamType" : [
            "private-crowd",
            "vendor-crowd"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DAXServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es DAX, Netzwerkschnittstelle, Sicherheitsgruppe, Subnetz und VPC im Namen des Kunden zu erstellen und zu verwalten

`DAXServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. März 2018, 17:51 UTC
- Bearbeitete Zeit: 5. März 2018, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DAXServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DeclarativePoliciesEC2Report

Beschreibung: Bietet Zugriff auf schreibgeschützte Dateien, die für die Ausführung des Kontostatusberichts mit EC2 deklarativen Richtlinien APIs erforderlich sind.

`DeclarativePoliciesEC2Report`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 30. November 2024, 13:21 UTC
- Bearbeitete Zeit: 30. November 2024, 13:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DeclarativePoliciesEC2Report`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DeclarativePoliciesEC2Report",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeRegions",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetAllowedImagesSettings",
        "ec2:DescribeVpcBlockPublicAccessOptions"
```

```
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBCloudWatchContributorInsightsServiceRolePolicy

Beschreibung: Für die Unterstützung von Amazon CloudWatch Contributor Insights for Amazon DynamoDB sind Berechtigungen erforderlich.

`DynamoDBCloudWatchContributorInsightsServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2019, 21:13 Uhr UTC
- Bearbeitete Zeit: 15. November 2019, 21:13 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBCloudWatchContributorInsightsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "cloudwatch:DeleteInsightRules",
        "cloudwatch:PutInsightRule"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:cloudwatch:*:*:insight-rule/DynamoDBContributorInsights*"
    },
    {
      "Action" : [
        "cloudwatch:DescribeInsightRules"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBGlobalTableSettingsManagementServiceRolePolicy

Beschreibung: Von DynamoDB benötigte Berechtigungen zur Verwaltung globaler Tabellenreplikateinstellungen

`DynamoDBGlobalTableSettingsManagementServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Oktober 2025, 17:34 UTC
- Zeit bearbeitet: 22. November 2025, 01:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBGlobalTableSettingsManagementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "DynamoDBActionsNeededToReplicateSettings",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget"
      ],
      "Resource" : [
        "arn:aws:application-autoscaling:*:*:scalable-target/*",
        "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/dynamodb/table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "application-autoscaling:service-namespace" : [
            "dynamodb"
          ]
        }
      }
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBKinesisReplicationServiceRolePolicy

Beschreibung: Bieten Sie AWS DynamoDB-Zugriff auf KinesisDataStreams

`DynamoDBKinesisReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. November 2020, 00:43 UTC
- Zeit bearbeitet: 12. November 2020, 00:43 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBKinesisReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "kinesis.*.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords",
        "kinesis:DescribeStream"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

DynamoDBReplicationServiceRolePolicy

Beschreibung: Von DynamoDB für die regionsübergreifende Datenreplikation benötigte Berechtigungen

`DynamoDBReplicationServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 9. November 2017, 23:55 UTC
- Bearbeitete Zeit: 8. Januar 2024, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/DynamoDBReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DynamoDBActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:UpdateItem",
        "dynamodb:DeleteItem",
        "dynamodb:DescribeTable",
        "dynamodb:UpdateTable",
        "dynamodb:Scan",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:UpdateTimeToLive",
        "dynamodb:DescribeLimits",
        "dynamodb:GetResourcePolicy",
```

```
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:DescribeScalingPolicies",
        "account:ListRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DynamoDBReplicationServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "dynamodb.application-autoscaling.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FastLaunchFullAccess

Beschreibung: Diese Richtlinie gewährt vollen Zugriff auf EC2 Fast Launch-Aktionen

`EC2FastLaunchFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `EC2FastLaunchFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 13. Mai 2024, 22:45 UTC
- Bearbeitete Zeit: 14. Mai 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2FastLaunchFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2FastLaunch",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableFastLaunch",
        "ec2:DisableFastLaunch",
        "ec2:DescribeFastLaunchImages"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2ReadOnly",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes",
        "ec2:DescribeRegions",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeTags",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAccountAttributes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2CreateVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ModifyDeleteVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:CreateSubnet",
        "ec2:ModifyVpcAttribute",
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
```

```
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2CreateSecurityGroup",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2ManageSecurityGroupEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CloudFormation",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:RollbackStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateTerminationProtection",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/EC2FastLaunch*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchTemplateModify",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyLaunchTemplate",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion"
      ],
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
```

```
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "EC2LaunchInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "EC2LaunchInstanceWithVolAndInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "EC2Tags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
```

```
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "RunInstances"
        }
      }
    },
    {
      "Sid" : "EC2ManageTags",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/ec2fastlaunch.amazonaws.com/
AWSServiceRoleForEC2FastLaunch",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "ec2fastlaunch.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMSLRPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FastLaunchServiceRolePolicy

Beschreibung: Die Richtlinie gewährt ec2fastlaunch die Möglichkeit, vorab bereitgestellte Snapshots im Kundenkonto vorzubereiten und zu verwalten und zugehörige Metriken zu veröffentlichen.

`EC2FastLaunchServiceRolePolicy`ist eine verwaltete AWS Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 10. Januar 2022, 13:08 UTC
- Bearbeitete Zeit: 18. Juli 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FastLaunchServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowRunInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*::image/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:aws:license-manager:*:*:license-configuration:*"
      ]
    },
    {
      "Sid" : "AllowRunInstancesOnFastLaunchCreatedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStopAndTerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTaggedSnapshot",
      "Effect" : "Allow",
      "Action" : "ec2:CreateSnapshot",
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        },
        "StringLike" : {
          "aws:RequestTag/CreatedByLaunchTemplateVersion" : "*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:TagKeys" : [
            "CreatedByLaunchTemplateName",
            "CreatedByLaunchTemplateId"
          ]
        }
      }
    },
    {
      "Sid" : "AllowCreateLaunchTemplate",
      "Effect" : "Allow",
      "Action" : "ec2:CreateLaunchTemplate",
      "Resource" : "arn:aws:ec2:*:*:launch-template/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowCreateTags",
```

```
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:launch-template/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSnapshot",
            "RunInstances",
            "CreateLaunchTemplate"
          ]
        }
      }
    },
    {
      "Sid" : "AllowDeleteSnapshots",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    },
    {
      "Sid" : "AllowDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeVolumes",
        "ec2:DescribeNetworkInterfaces",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPutMetricData",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/EC2"
        }
      }
    },
    {
      "Sid" : "AllowEventsRuleMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:RemoveTargets",
        "events:PutRule",
        "events:PutTargets"
      ],
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "ec2fastlaunch.amazonaws.com"
        }
      },
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowEventsRuleNonMutations",
      "Effect" : "Allow",
      "Action" : [
        "events:ListTargetsByRule",
        "events:DescribeRule"
      ],
      "Resource" : [
        "arn:aws:events:*:*:rule/FastLaunch*"
      ]
    },
    {
      "Sid" : "AllowKMSActions",
      "Effect" : "Allow",
      "Action" : "kms:ListRetirableGrants",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowDeleteFastLaunchLaunchTemplates",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteLaunchTemplate"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Fast Launch"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2FleetTimeShiftableServiceRolePolicy

Beschreibung: Richtlinie, die EC2 Fleet die Erlaubnis erteilt, Instances in future zu starten.

`EC2FleetTimeShiftableServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 23. Dezember 2019, 19:47 UTC
- Bearbeitete Zeit: 23. Dezember 2019, 19:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EC2FleetTimeShiftableServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstances",
        "ec2:RunInstances",
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com",
            "ec2.amazonaws.com.cn"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:spot-instances-request/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:ec2:fleet-id" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Ec2ImageBuilderCrossAccountDistributionAccess

Beschreibung: EC2 Image Builder benötigt Berechtigungen, um eine kontoübergreifende Verteilung durchzuführen.

`Ec2ImageBuilderCrossAccountDistributionAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `Ec2ImageBuilderCrossAccountDistributionAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. September 2020, 19:22 UTC
- Bearbeitete Zeit: 30. September 2020, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/Ec2ImageBuilderCrossAccountDistributionAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*::image/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2ImageBuilderLifecycleExecutionPolicy

Beschreibung: Die EC2 ImageBuilderLifecycleExecutionPolicy Richtlinie gewährt Image Builder die Erlaubnis, Aktionen wie das Verwerfen oder Löschen von Image Builder Builder-Image-Ressourcen und den ihnen zugrunde liegenden Ressourcen (AMIs, Snapshots) auszuführen, um automatisierte Regeln für Image-Lebenszyklusverwaltungsaufgaben zu unterstützen.

`EC2ImageBuilderLifecycleExecutionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `EC2ImageBuilderLifecycleExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 16. November 2023, 23:23 UTC
- Bearbeitete Zeit: 16. November 2023, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/EC2ImageBuilderLifecycleExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Ec2ImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:EnableImage",
        "ec2:DeregisterImage",
        "ec2:EnableImageDeprecation",
        "ec2:DescribeImageAttribute",
        "ec2:DisableImage",
        "ec2:DisableImageDeprecation"
      ],
      "Resource" : "arn:aws:ec2:*::image/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2DeleteSnapshotPermission",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteSnapshot",
      "Resource" : "arn:aws:ec2:*::snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "EC2TagsPermission",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*::image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/DeprecatedBy" : "EC2 Image Builder",
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "DeprecatedBy"
        }
      }
    },
    {
      "Sid" : "ECRImagePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:BatchDeleteImage"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "ecr:ResourceTag/LifecycleExecutionAccess" : "EC2 Image Builder"
        }
      }
    },
    {
      "Sid" : "ImageBuilderEC2TagServicePermission",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "tag:GetResources",
        "imagebuilder:DeleteImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceConnect

Beschreibung: Ermöglicht Kunden, EC2 Instance Connect aufzurufen, um kurzlebige Schlüssel für ihre EC2 Instances zu veröffentlichen und Connect über SSH oder die EC2 Instance Connect-CLI herzustellen.

`EC2InstanceConnect`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `EC2InstanceConnect` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. Juni 2019, 18:53 UTC
- Bearbeitete Zeit: 27. Juni 2019, 18:53 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceConnect`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2InstanceConnect",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Ec2InstanceConnectEndpoint

Beschreibung: EC2 Instance Connect-Endpunktrichtlinie zur Verwaltung von EC2 Instance Connect-Endpunkten, die vom Kunden erstellt wurden

`Ec2InstanceConnectEndpoint`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. Januar 2023, 20:19 UTC
- Bearbeitete Zeit: 31. Juli 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Ec2InstanceConnectEndpoint`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "InstanceConnectEndpointId"
          ]
        },
```

```
        "StringLike" : {
          "aws:RequestTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:ModifyNetworkInterfaceAttribute",
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/InstanceConnectEndpointId" : [
            "eice-*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceProfileForImageBuilder

Beschreibung: EC2 Instanzprofil für den Image Builder Builder-Dienst.

`EC2InstanceProfileForImageBuilder`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `EC2InstanceProfileForImageBuilder` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. Dezember 2019, 19:08 Uhr UTC
- Bearbeitete Zeit: 19. Mai 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilder`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedBy" : "EC2 Image Builder"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateSnapshot",
          "aws:RequestTag/CreatedBy" : [
            "EC2 Image Builder"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/*.ISO",
        "arn:aws:s3:::*/*.iso",
        "arn:aws:s3:::*/*.Iso"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetMarketplaceResource"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EC2InstanceProfileForImageBuilderECRContainerBuilds

Beschreibung: EC2 Instanzprofil für die Erstellung von Container-Images mit EC2 Image Builder. Diese Richtlinie gewährt dem Benutzer umfassende Rechte zum Hochladen von ECR-Bildern.

`EC2InstanceProfileForImageBuilderECRContainerBuilds`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `EC2InstanceProfileForImageBuilderECRContainerBuilds` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Dezember 2020, 19:48 UTC
- Bearbeitete Zeit: 11. Dezember 2020, 19:48 UTC
- ARN: `arn:aws:iam::aws:policy/EC2InstanceProfileForImageBuilderECRContainerBuilds`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:InitiateLayerUpload",
        "ecr:UploadLayerPart",
        "ecr:CompleteLayerUpload",
        "ecr:BatchCheckLayerAvailability",
```

```
        "ecr:GetDownloadUrlForLayer",
        "ecr:PutImage"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:imagebuilder:arn",
          "aws:CalledVia" : [
            "imagebuilder.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "arn:aws:s3:::ec2imagebuilder*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/imagebuilder/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ECRReplicationServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von ECR Replication verwendet oder verwaltet werden

`ECRReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 4. Dezember 2020, 22:11 Uhr UTC
- Bearbeitete Zeit: 4. Dezember 2020, 22:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository",
        "ecr:ReplicateImage"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ECRTemplateServiceRolePolicy

Beschreibung: Ermöglicht die Ausführung von Aktionen bei der Verwendung von Vorlagen zur Erstellung von AWS ECR-Repositorys

`ECRTemplateServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 19. Juni 2024, 23:11 UTC
- Bearbeitete Zeit: 19. Juni 2024, 23:11 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ECRTemplateServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateRepositoryWithTemplate",
      "Effect" : "Allow",
      "Action" : [
        "ecr:CreateRepository"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElastiCacheServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es ElastiCache , AWS Ressourcen in Ihrem Namen zu verwalten, sofern dies für die Verwaltung Ihres Caches erforderlich ist

`ElastiCacheServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. Dezember 2017, 17:50 Uhr UTC
- Bearbeitete Zeit: 28. November 2023, 03:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ElastiCacheServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ElastiCacheManagementActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:RevokeSecurityGroupIngress",
        "cloudwatch:PutMetricData",
        "outposts:GetOutpost",
        "outposts:GetOutpostInstanceTypes",
        "outposts:ListOutposts",
        "outposts:ListSites"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateDeleteVPCEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringLike" : {
          "ec2:VpceServiceName" : "com.amazonaws.elasticache.serverless.*"
        }
      }
    },
    {
      "Sid" : "TagVPCEndpointsOnCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint",
          "aws:RequestTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVpcEndpoints",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonElastiCacheManaged" : "true"
        }
      }
    },
    {
      "Sid" : "AllowAccessToElastiCacheTaggedVpcEndpoints",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint",
        "ec2:ModifyVpcEndpoint"
      ],
      "NotResource" : "arn:aws:ec2:*:*:vpc-endpoint/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElasticLoadBalancingFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon und eingeschränkten Zugriff auf andere Dienste ElasticLoadBalancing, die für die Bereitstellung von ElasticLoadBalancing Funktionen erforderlich sind.

`ElasticLoadBalancingFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElasticLoadBalancingFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2018, 20:42 UTC
- Bearbeitete Zeit: 24. Oktober 2024, 22:21 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingFullAccess`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "elasticloadbalancing:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeClassicLinkInstances",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:DescribeVpcPeeringConnections",
        "cognito-idp:DescribeUserPoolClient"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:*",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElasticLoadBalancingReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon ElasticLoadBalancing und abhängige Dienste

`ElasticLoadBalancingReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElasticLoadBalancingReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. September 2018, 20:17 Uhr UTC
- Bearbeitete Zeit: 26. November 2023, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/ElasticLoadBalancingReadOnly`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "Statement1",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:Describe*",
```

```
        "elasticloadbalancing:Get*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Statement3",
      "Effect" : "Allow",
      "Action" : "arc-zonal-shift:GetManagedResource",
      "Resource" : "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    },
    {
      "Sid" : "Statement4",
      "Effect" : "Allow",
      "Action" : [
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsDownloadSoftwareAccess

Beschreibung: Zugriff auf gekaufte Ressourcen und Herunterladen der zugehörigen Software und Kickstart-Dateien

`ElementalActivationsDownloadSoftwareAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalActivationsDownloadSoftwareAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 8. September 2020, 17:26 Uhr UTC
- Bearbeitete Zeit: 8. September 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsDownloadSoftwareAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
```

```
        "elemental-activations:Download*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsFullAccess

Beschreibung: Vollständiger Zugriff, um die von Elemental Appliances und Software gekauften Ressourcen einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalActivationsFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalActivationsFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. Juni 2020, 21:00 Uhr UTC
- Bearbeitete Zeit: 4. Juni 2020, 21:00 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsGenerateLicenses

Beschreibung: Zugriff auf gekaufte Ressourcen und Generierung von Softwarelizenzen für ausstehende Aktivierungen

`ElementalActivationsGenerateLicenses`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalActivationsGenerateLicenses` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2020, 18:28 Uhr UTC
- Zeit bearbeitet: 28. August 2020, 18:28 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsGenerateLicenses`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*",
        "elemental-activations:GenerateLicenses",
        "elemental-activations:StartFileUpload",
        "elemental-activations:CompleteFileUpload"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalActivationsReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff auf die detaillierte Liste der gekauften Vermögenswerte, die dem AWS-Konto Benutzer zugeordnet sind

`ElementalActivationsReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalActivationsReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 28. August 2020, 16:51 UTC
- Zeit bearbeitet: 28. August 2020, 16:51 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalActivationsReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-activations:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalAppliancesSoftwareFullAccess

Beschreibung: Vollständiger Zugriff, um Angebote und Bestellungen von Elemental Appliances und Software einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalAppliancesSoftwareFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalAppliancesSoftwareFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 31. Juli 2019, 16:28 UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:01 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalAppliancesSoftwareReadOnlyAccess

Beschreibung: Schreibgeschützter Zugriff, um Angebote und Bestellungen von Elemental Appliances und Software einzusehen

`ElementalAppliancesSoftwareReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `ElementalAppliancesSoftwareReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 1. April 2020, 22:31 UTC
- Bearbeitete Zeit: 1. April 2020, 22:31 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalAppliancesSoftwareReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-appliances-software:List*",
        "elemental-appliances-software:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ElementalSupportCenterFullAccess

Beschreibung: Uneingeschränkter Zugriff, um Support-Anfragen und Inhalte zum Produktsupport von Elemental Appliance und Software einzusehen und entsprechende Maßnahmen zu ergreifen

`ElementalSupportCenterFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ElementalSupportCenterFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. November 2020, 18:08 Uhr UTC
- Bearbeitete Zeit: 5. Februar 2021, 21:02 UTC
- ARN: `arn:aws:iam::aws:policy/ElementalSupportCenterFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elemental-support-cases:*",
        "elemental-support-content:*",
        "elemental-activations:CompleteAccountRegistration"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

EMRDescribeClusterPolicyForEMRWAL

Beschreibung: Diese Richtlinie gewährt Nur-Lese-Berechtigungen, die es dem WAL-Service für Amazon EMR ermöglichen, den Status eines Clusters zu finden und zurückzugeben.

`EMRDescribeClusterPolicyForEMRWAL`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Juni 2023, 23:30 UTC
- Bearbeitete Zeit: 15. Juni 2023, 23:30 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/EMRDescribeClusterPolicyForEMRWAL`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

FMSServiceRolePolicy

Beschreibung: Zugriffsrichtlinie, die es der Rolle ermöglicht, FM-bezogene Aktionen für FM-verwaltete Ressourcen innerhalb eines Kundenorganisationskontos durchzuführen. AWS

`FMSServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. März 2018, 23:01 UTC
- Bearbeitete Zeit: 21. Mai 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FMSServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v32 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WafGeneral",
      "Effect" : "Allow",
      "Action" : [
        "waf:UpdateWebACL",
```

```
        "waf:DeleteWebACL",
        "waf:GetWebACL",
        "waf:GetRuleGroup",
        "waf:ListSubscribedRuleGroups",
        "waf-regional:UpdateWebACL",
        "waf-regional:DeleteWebACL",
        "waf-regional:GetWebACL",
        "waf-regional:GetRuleGroup",
        "waf-regional:ListSubscribedRuleGroups",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:AssociateWebACL",
        "waf-regional:DisassociateWebACL",
        "elasticloadbalancing:SetWebACL",
        "apigateway:SetWebACL",
        "elasticloadbalancing:SetSecurityGroups",
        "waf:ListTagsForResource",
        "waf-regional:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:rulegroup/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*",
        "arn:aws:apigateway:*::/restapis/*/stages/*"
      ]
    },
    {
      "Sid" : "Wafv2Logging",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/webacl/*"
      ]
    },
    {
      "Sid" : "WafWebaclCreation",
      "Effect" : "Allow",
```

```
      "Action" : [
        "waf:CreateWebACL",
        "waf-regional:CreateWebACL",
        "waf:GetChangeToken",
        "waf-regional:GetChangeToken",
        "waf-regional:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:*",
        "arn:aws:waf-regional:*:*:*"
      ]
    },
    {
      "Sid" : "ElbGeneral",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:DescribeTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "WafPermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "waf:PutPermissionPolicy",
        "waf:GetPermissionPolicy",
        "waf:DeletePermissionPolicy",
        "waf-regional:PutPermissionPolicy",
        "waf-regional:GetPermissionPolicy",
        "waf-regional:DeletePermissionPolicy"
      ],
      "Resource" : [
        "arn:aws:waf:*:*:webacl/*",
        "arn:aws:waf:*:*:rulegroup/*",
        "arn:aws:waf-regional:*:*:webacl/*",
        "arn:aws:waf-regional:*:*:rulegroup/*"
      ]
    },
    {
      "Sid" : "CloudfrontGeneral",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution",
```

```
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "cloudfront:AssociateDistributionWebACL",
        "cloudfront:DisassociateDistributionWebACL"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ConfigScoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DeleteConfigRule",
        "config:GetComplianceDetailsByConfigRule",
        "config:PutConfigRule",
        "config:StartConfigRulesEvaluation",
        "config:DeleteEvaluationResults"
      ],
      "Resource" : "arn:aws:config:*:*:config-rule/aws-service-rule/fms.amazonaws.com/
*"
    },
    {
      "Sid" : "ConfigUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeComplianceByConfigRule",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRules",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:PutConfigurationRecorder",
        "config:StartConfigurationRecorder",
        "config:PutDeliveryChannel",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetComplianceSummaryByConfigRule",
        "config:GetDiscoveredResourceCounts",
        "config:PutEvaluations",
        "config:SelectResourceConfig",
        "config:BatchGetResourceConfig"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "SlrDeletion",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/fms.amazonaws.com/AWSServiceRoleForFMS"
      ]
    },
    {
      "Sid" : "OrganizationsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ShieldGeneral",
      "Effect" : "Allow",
      "Action" : [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:ListAttacks",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",
        "shield:GetSubscriptionState",
        "shield:DescribeDRTAccess",
        "shield:DescribeEmergencyContactSettings",
        "shield:UpdateEmergencyContactSettings",
```

```
        "elasticloadbalancing:DescribeLoadBalancers",
        "ec2:DescribeAddresses",
        "shield:EnableApplicationLayerAutomaticResponse",
        "shield:DisableApplicationLayerAutomaticResponse",
        "shield:UpdateApplicationLayerAutomaticResponse"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2SecurityGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Sid" : "SecurityGroupTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    },
    {
      "Sid" : "SecurityGroupTagManagement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/FMManaged" : "*"
        }
      }
    },
    {
      "Sid" : "Ec2Unscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeInstances",
        "ec2:AssociateRouteTable",
        "ec2:CreateSubnet",
        "ec2:CreateRouteTable",
        "ec2:DeleteSubnet",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Wafv2General",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:TagResource",
        "wafv2:ListResourcesForWebACL",
```

```
        "wafv2:AssociateWebACL",
        "wafv2:ListTagsForResource",
        "wafv2:UntagResource",
        "wafv2:GetWebACL",
        "wafv2:DisassociateFirewallManager",
        "wafv2:DeleteWebACL",
        "wafv2:DisassociateWebACL"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "Wafv2WebAclAndRuleGroupMutation",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:UpdateWebACL",
        "wafv2:CreateWebACL",
        "wafv2:DeleteFirewallManagerRuleGroups",
        "wafv2:PutFirewallManagerRuleGroups"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:global/webacl/*",
        "arn:aws:wafv2:*:*:regional/webacl/*",
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/ipset/*",
        "arn:aws:wafv2:*:*:regional/ipset/*",
        "arn:aws:wafv2:*:*:global/regexpatternset/*",
        "arn:aws:wafv2:*:*:regional/regexpatternset/*"
      ]
    },
    {
      "Sid" : "Wafv2PermissionPolicy",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutPermissionPolicy",
        "wafv2:GetPermissionPolicy",
        "wafv2:DeletePermissionPolicy"
      ],
      "Resource" : [
```

```
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*"
      ]
    },
    {
      "Sid" : "Wafv2WebaclDescribe",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:GetWebACLForResource"
      ],
      "Resource" : [
        "arn:aws:wafv2:*:*:regional/webacl/*"
      ]
    },
    {
      "Sid" : "RouteTableTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateRouteTable"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "SubnetTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "VPCEndpointTagManagement",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateVpcEndpoint"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RouteTableCleanup",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteRouteTable",
      "Resource" : "arn:aws:ec2:*:*:route-table/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeAvailabilityZones"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CreateVpcEndpointScoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
        }
      }
    },
    {
      "Sid" : "CreateVpcEndpointUnscoped",
      "Effect" : "Allow",
      "Action" : "ec2:CreateVpcEndpoint",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VpcEndpointsDeletion",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ram:TagResource"
```

```
      ],
      "Resource" : [
        "arn:aws:ram:*:*:resource-share/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        }
      }
    },
    {
      "Sid" : "RamMutation",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:UpdateResourceShare",
        "ram:DeleteResourceShare"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RamCreation",
      "Effect" : "Allow",
      "Action" : "ram:CreateResourceShare",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : [
            "true"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "RamDescribe",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SlrCreation",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "network-firewall.amazonaws.com",
            "shield.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamDescribe",
      "Effect" : "Allow",
      "Action" : "iam:GetRole",
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "NetworkFirewallGeneral",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:AssociateSubnets",
        "network-firewall:CreateFirewall",
        "network-firewall:CreateFirewallPolicy",
        "network-firewall:DisassociateSubnets",
        "network-firewall:UpdateFirewallDeleteProtection",
        "network-firewall:UpdateFirewallPolicy",
        "network-firewall:UpdateFirewallPolicyChangeProtection",
        "network-firewall:UpdateSubnetChangeProtection",
        "network-firewall:AssociateFirewallPolicy",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DeleteResourcePolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:UpdateLoggingConfiguration",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListTLSInspectionConfigurations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "NetworkFirewallResourcePolicy",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:firewall-policy/*",
        "arn:aws:network-firewall:*:*:stateful-rulegroup/*",
        "arn:aws:network-firewall:*:*:stateless-rulegroup/*"
      ]
    },
```

```
    {
      "Sid" : "NetworkFirewallCleanup",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:DeleteFirewallPolicy",
        "network-firewall:DeleteFirewall"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "LogsGeneral",
      "Effect" : "Allow",
      "Action" : [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:ListFirewallRuleGroupAssociations",
        "route53resolver:ListTagsForResource",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroupAssociation",
        "route53resolver:GetFirewallRuleGroup",
        "route53resolver:GetFirewallRuleGroupPolicy",
        "route53resolver:PutFirewallRuleGroupPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53ResolverRuleGroupCleanup",
      "Effect" : "Allow",
      "Action" : [
```

```
        "route53resolver:UpdateFirewallRuleGroupAssociation",
        "route53resolver:DisassociateFirewallRuleGroup"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "Route53ResolverRuleGroupScoped",
      "Effect" : "Allow",
      "Action" : [
        "route53resolver:AssociateFirewallRuleGroup",
        "route53resolver:TagResource"
      ],
      "Resource" : "arn:aws:route53resolver:*:*:firewall-rule-group-association/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclTagCreation",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkAcl"
        }
      }
    },
```

```
    {
      "Sid" : "NaclTagManagement",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-acl/*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "Name",
            "FMManaged",
            "FMPolicies"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclScoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkAclEntry",
        "ec2:CreateNetworkAclEntry",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:DeleteNetworkAcl"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/FMManaged" : "true"
        }
      }
    },
    {
      "Sid" : "NaclUnscoped",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:DescribeNetworkAcls",
        "ec2:CreateNetworkAcl"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

FSxDeleteServiceLinkedRoleAccess

Beschreibung: Ermöglicht Amazon FSx , seine Service Linked Roles für den Amazon S3 S3-Zugriff zu löschen

`FSxDeleteServiceLinkedRoleAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. November 2018, 10:40 Uhr UTC
- Zeit bearbeitet: 28. November 2018, 10:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/FSxDeleteServiceLinkedRoleAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:GetRole"
      ],
      "Resource" : "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GameLiftContainerFleetPolicy

Beschreibung: Gewährt die erforderlichen Berechtigungen für Rechenaktionen in einer GameLift Amazon-Containerflotte, einschließlich des Zugriffs auf Abhängigkeiten wie Amazon S3.

`GameLiftContainerFleetPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GameLiftContainerFleetPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 12. November 2024, 19:28 UTC
- Zeit bearbeitet: 5. Februar 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftContainerFleetPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "WriteGameSessionLogsToLogStream",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*:log-stream:*"
    },
    {
      "Sid" : "CreateLogGroupToStoreGameSessionLogs",
      "Effect" : "Allow",
      "Action" : "logs:CreateLogGroup",
      "Resource" : "arn:aws:logs:*:*:log-group:gamelift-*"
    },
    {
      "Sid" : "WriteGameSessionLogsToS3Bucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource" : [
        "arn:aws:s3:::gamelift-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RetrieveComputeAuthToken",
      "Effect" : "Allow",
      "Action" : [
        "gamelift:GetComputeAuthToken"
      ],
      "Resource" : [
        "arn:aws:gamelift:*:*:containerfleet/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GameLiftGameServerGroupPolicy

Beschreibung: Richtlinie, die es Gamelift ermöglicht, Kundenressourcen GameServerGroups zu verwalten

`GameLiftGameServerGroupPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GameLiftGameServerGroupPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. April 2020, 23:12 UTC
- Bearbeitete Zeit: 13. Mai 2020, 17:27 UTC
- ARN: `arn:aws:iam::aws:policy/GameLiftGameServerGroupPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "ec2:TerminateInstances",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:CompleteLifecycleAction",
        "autoscaling:ResumeProcesses",
```

```
        "autoscaling:EnterStandby",
        "autoscaling:SetInstanceProtection",
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:SuspendProcesses",
        "autoscaling:DetachInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/GameLift" : "GameServerGroups"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "autoscaling:DescribeAutoScalingGroups",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSubnets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sns:Publish",
      "Resource" : [
        "arn:*:sns:*:*:ActivatingLifecycleHookTopic-*",
        "arn:*:sns:*:*:TerminatingLifecycleHookTopic-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/GameLift"
        }
      }
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GitLabDuoWithAmazonQPermissionsPolicy

Beschreibung: Diese verwaltete Richtlinie gewährt die Erlaubnis, eine Verbindung mit Amazon Q herzustellen und die Funktionen der GitLab Duo with Amazon Q-Integration zu nutzen.

`GitLabDuoWithAmazonQPermissionsPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GitLabDuoWithAmazonQPermissionsPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 16. April 2025, 16:37 UTC
- Bearbeitete Zeit: 16. April 2025, 16:37 UTC
- ARN: `arn:aws:iam::aws:policy/GitLabDuoWithAmazonQPermissionsPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GitLabDuoUsagePermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:SendEvent",
        "q:CreateAuthGrant",
        "q:UpdateAuthGrant",
        "q:GenerateCodeRecommendations",
        "q:SendMessage",
        "q:ListPlugins",
        "q:VerifyOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreateOAuthAppConnection",
        "q:DeleteOAuthAppConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GitLabDuoPluginPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:CreatePlugin",
        "q:DeletePlugin",
        "q:GetPlugin"
      ],
      "Resource" : "arn:aws:qdeveloper:*:*:plugin/GitLabDuoWithAmazonQ/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GlobalAcceleratorFullAccess

Beschreibung: Erlauben Sie GlobalAccelerator Benutzern vollen Zugriff auf alle APIs

`GlobalAcceleratorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GlobalAcceleratorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 02:44 Uhr UTC
- Zeit bearbeitet: 4. Dezember 2020, 19:17 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "globalaccelerator:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "elasticloadbalancing:DescribeLoadBalancers",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRegions",
        "ec2:DescribeSubnets"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "globalaccelerator.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GlobalAcceleratorReadOnlyAccess

Beschreibung: GlobalAccelerator Benutzern nur Lesezugriff gewähren APIs

`GlobalAcceleratorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GlobalAcceleratorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 02:41 UTC
- Zeit bearbeitet: 27. November 2018, 02:41 UTC
- ARN: `arn:aws:iam::aws:policy/GlobalAcceleratorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Action" : [
        "globalaccelerator:Describe*",
        "globalaccelerator:List*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GreengrassOTAUpdateArtifactAccess

Beschreibung: Bietet Lesezugriff auf die Greengrass OTA Update-Artefakte in allen Greengrass-Regionen

`GreengrassOTAUpdateArtifactAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GreengrassOTAUpdateArtifactAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 29. November 2017, 18:11 Uhr UTC
- Bearbeitete Zeit: 18. Dezember 2018, 00:59 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/GreengrassOTAUpdateArtifactAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowsIotToAccessGreengrassOTAUpdateArtifacts",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-greengrass-updates/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GroundTruthSyntheticConsoleFullAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen, die für die Nutzung aller Funktionen der SageMaker Ground Truth Synthetic Console erforderlich sind.

`GroundTruthSyntheticConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GroundTruthSyntheticConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. August 2022, 15:58 Uhr UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

GroundTruthSyntheticConsoleReadOnlyAccess

Beschreibung: Diese Richtlinie gewährt nur Lesezugriff auf SageMaker Ground Truth Synthetic über die. AWS-Managementkonsole

`GroundTruthSyntheticConsoleReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `GroundTruthSyntheticConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 25. August 2022, 15:58 Uhr UTC
- Bearbeitete Zeit: 25. August 2022, 15:58 UTC
- ARN: `arn:aws:iam::aws:policy/GroundTruthSyntheticConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-groundtruth-synthetic:List*",
        "sagemaker-groundtruth-synthetic:Get*",
        "s3:ListBucket"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Health_OrganizationsServiceRolePolicy

Beschreibung: AWS Gesundheitsrichtlinie zur Aktivierung der Funktion Organizational View

`Health_OrganizationsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Dezember 2019, 13:28 Uhr UTC
- Bearbeitete Zeit: 6. Februar 2024, 16:07 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Health_OrganizationsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "HealthAPIOrganizationView0",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAdvisorReadOnly

Beschreibung: Diese Richtlinie gewährt Lesezugriff auf alle vom IAM Access Advisor bereitgestellten Zugriffsinformationen, z. B. Informationen über den Dienst, auf den zuletzt zugegriffen wurde.

`IAMAccessAdvisorReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMAccessAdvisorReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 21. Juni 2019, 19:33 UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:33 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAdvisorReadOnly`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:ListUsers",
        "iam:ListGroups",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:GenerateOrganizationsAccessReport",
        "iam:GenerateCredentialReport",
        "iam:GetRole",
        "iam:GetPolicy",
        "iam:GetServiceLastAccessedDetails",
        "iam:GetServiceLastAccessedDetailsWithEntities",
        "iam:GetOrganizationsAccessReport",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAnalyzerFullAccess

Beschreibung: Bietet vollen Zugriff auf IAM Access Analyzer

`IAMAccessAnalyzerFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMAccessAnalyzerFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2019, 17:12 Uhr UTC
- Bearbeitete Zeit: 2. Dezember 2019, 17:12 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:*"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "access-analyzer.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMAccessAnalyzerReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IAM Access Analyzer-Ressourcen

`IAMAccessAnalyzerReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMAccessAnalyzerReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 2. Dezember 2019, 17:12 Uhr UTC
- Bearbeitete Zeit: 18. Juli 2024, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/IAMAccessAnalyzerReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IAMAccessAnalyzerReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "access-analyzer:CheckAccessNotGranted",
        "access-analyzer:CheckNoNewAccess",
        "access-analyzer:CheckNoPublicAccess",
        "access-analyzer:Get*",
        "access-analyzer:List*",
        "access-analyzer:ValidatePolicy"
      ],
```

```
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMFullAccess

Beschreibung: Bietet vollen Zugriff auf IAM über die AWS-Managementkonsole.

`IAMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 Uhr UTC
- Bearbeitete Zeit: 21. Juni 2019, 19:40 UTC
- ARN: `arn:aws:iam::aws:policy/IAMFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:*",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribePolicy",
        "organizations:ListChildren",
        "organizations:ListParents",
        "organizations:ListPoliciesForTarget",
        "organizations:ListRoots",
        "organizations:ListPolicies",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IAM über die AWS-Managementkonsole.

`IAMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:40 UTC
- Bearbeitete Zeit: 25. Januar 2018, 19:11 UTC
- ARN: `arn:aws:iam::aws:policy/IAMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource" : "*"
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMSelfManageServiceSpecificCredentials

Beschreibung: Ermöglicht es einem IAM-Benutzer, seine eigenen dienstspezifischen Anmeldeinformationen zu verwalten.

`IAMSelfManageServiceSpecificCredentialsist` eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMSelfManageServiceSpecificCredentials` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. Dezember 2016, 17:25 Uhr UTC
- Bearbeitete Zeit: 22. Dezember 2016, 17:25 UTC
- ARN: `arn:aws:iam::aws:policy/IAMSelfManageServiceSpecificCredentials`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceSpecificCredential",
        "iam:ListServiceSpecificCredentials",
        "iam:UpdateServiceSpecificCredential",
        "iam:DeleteServiceSpecificCredential",
        "iam:ResetServiceSpecificCredential"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMUserChangePassword

Beschreibung: Bietet einem IAM-Benutzer die Möglichkeit, sein eigenes Passwort zu ändern.

`IAMUserChangePassword`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMUserChangePassword` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 15. November 2016, 00:25 UTC
- Bearbeitete Zeit: 29. Mai 2025, 21:52 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserChangePassword`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:ChangePassword"
      ],
      "Resource" : [
        "arn:aws:iam::*:user/${aws:username}",
        "arn:aws:iam::*:user/*/${aws:username}"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetAccountPasswordPolicy"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IAMUserSSHKeys

Beschreibung: Bietet IAM-Benutzern die Möglichkeit, ihre eigenen SSH-Schlüssel zu verwalten.

`IAMUserSSHKeys`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IAMUserSSHKeys` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 9. Juli 2015, 17:08 UTC
- Bearbeitete Zeit: 9. Juli 2015, 17:08 UTC
- ARN: `arn:aws:iam::aws:policy/IAMUserSSHKeys`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteSSHPublicKey",
        "iam:GetSSHPublicKey",
        "iam:ListSSHPublicKeys",
        "iam:UpdateSSHPublicKey",
        "iam:UploadSSHPublicKey"
      ],
      "Resource" : "arn:aws:iam::*:user/${aws:username}"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSFullAccess

Beschreibung: Bietet vollen Zugriff auf den Interactive Video Service (IVS). Enthält auch Berechtigungen für abhängige Dienste, die für den vollständigen Zugriff auf die IVS-Konsole erforderlich sind.

`IVSFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `IVSFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 13. Dezember 2023, 21:20 UTC
- Bearbeitete Zeit: 13. Dezember 2023, 21:20 UTC
- ARN: `arn:aws:iam::aws:policy/IVSFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:*",
        "ivschat:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf IVS-Streaming mit niedriger Latenz und Echtzeit-Streaming APIs

`IVSReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `IVSReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 5. Dezember 2023, 18:00 Uhr UTC
- Bearbeitete Zeit: 24. Juli 2025, 20:22 UTC
- ARN: `arn:aws:iam::aws:policy/IVSReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "IVSReadOnlyAccess",
      "Effect" : "Allow",
      "Action" : [
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
```

```
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipants",
        "ivs:ListParticipantReplicas",
        "ivs:ListParticipantEvents",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStages",
        "ivs:ListStageSessions",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreams",
        "ivs:ListStreamSessions",
        "ivs:ListTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

IVSRecordToS3

Beschreibung: Mit dem Service verknüpfte Rolle zur Ausführung von S3 PutObject zur Aufzeichnung von IVS-Livestreams

`IVSRecordToS3`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Dezember 2020, 00:10 UTC
- Bearbeitete Zeit: 5. Dezember 2020, 00:10 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/IVSRecordToS3`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::AWSIVS_*/ivs/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KafkaConnectServiceRolePolicy

Beschreibung: Diese Richtlinie gewährt Kafka Connect die Erlaubnis, AWS Ressourcen in Ihrem Namen zu verwalten.

`KafkaConnectServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. September 2021, 13:12 UTC
- Bearbeitete Zeit: 7. September 2021, 13:12 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaConnectServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonMSKConnectManaged" : "true"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "AmazonMSKConnectManaged"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMSKConnectManaged" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KafkaServiceRolePolicy

Beschreibung: Richtlinie für verknüpfte Rollen mit dem IAM-Dienst für Kafka.

`KafkaServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. November 2018, 23:31 UTC
- Zeit bearbeitet: 10. November 2025, 23:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KafkaServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:AttachNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DescribeVpcEndpoints",
        "acm-pca:GetCertificateAuthorityCertificate",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
```

```
      ],
      "Resource" : "arn:*:ec2:*:*:subnet/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : "arn:*:ec2:*:*:vpc-endpoint/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:DescribeSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "secretsmanager:SecretId" : "arn:*:secretsmanager:*:*:secret:AmazonMSK_*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssignIpv6Addresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:*:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:ResourceTag/AWSMSKManaged" : "true"
        },
        "StringLike" : {
          "ec2:ResourceTag/ClusterArn" : "*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KeyspacesCDCServiceRolePolicy

Beschreibung: Erteilt Amazon Keyspaces die erforderlichen Berechtigungen für Change Data Capture

`KeyspacesCDCServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 21. Juni 2025, 00:22 UTC
- Bearbeitungszeit: 21. Juni 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesCDCServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/Cassandra"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

KeyspacesReplicationServiceRolePolicy

Beschreibung: Von Keyspaces für die regionsübergreifende Datenreplikation benötigte Berechtigungen

`KeyspacesReplicationServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2023, 16:15 UTC
- Bearbeitete Zeit: 15. November 2024, 20:55 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/KeyspacesReplicationServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "KeyspacesActionsNeededForSteadyStateReplication",
      "Effect" : "Allow",
      "Action" : [
        "cassandra:Select",
        "cassandra:Modify",
        "cassandra:Alter",
        "cassandra:ModifyMultiRegionResource",
        "cassandra:SelectMultiRegionResource",
        "cassandra:AlterMultiRegionResource",
```

```
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CWDeleteAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*"
    },
    {
      "Sid" : "CWDescribeAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:*"
    },
    {
      "Sid" : "CWPutMetricAlarmPolicy",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking-*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "cloudwatch:AlarmActions" : [
            "arn:aws:autoscaling:*:*:scalingPolicy:*:resource/cassandra/keyspace/*/
table/*:policyName/*:createdBy/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LakeFormationDataAccessServiceRolePolicy

Beschreibung: Richtlinie zur Gewährung von temporärem Datenzugriff auf Lake Formation Formation-Ressourcen

`LakeFormationDataAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 20. Juni 2019, 20:46 UTC
- Bearbeitete Zeit: 6. Februar 2024, 18:37 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LakeFormationDataAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "LakeFormationDataAccessServiceRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LexBotPolicy

Beschreibung: Richtlinie für den AWS Lex Bot-Anwendungsfall

`LexBotPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 17. Februar 2017, 22:18 Uhr UTC
- Zeit bearbeitet: 13. November 2019, 22:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexBotPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "polly:SynthesizeSpeech"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "comprehend:DetectSentiment"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LexChannelPolicy

Beschreibung: Richtlinie für den AWS Lex Channel-Anwendungsfall

`LexChannelPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. Februar 2017, 23:23 Uhr UTC
- Zeit bearbeitet: 17. Februar 2017, 23:23 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LexChannelPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "lex:PostText"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

LightsailExportAccess

Beschreibung: Mit dem AWS Lightsail-Service verknüpfte Rollenrichtlinie, die Berechtigungen zum Exportieren von Ressourcen gewährt

`LightsailExportAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 28. September 2018, 16:35 Uhr UTC
- Bearbeitete Zeit: 15. Januar 2022, 01:45 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/LightsailExportAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:CopyImage",
        "ec2:DescribeImages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MediaConnectGatewayInstanceRolePolicy

Beschreibung: Diese Richtlinie gewährt die Erlaubnis, MediaConnect Gateway-Instances auf einem MediaConnect Gateway zu registrieren.

`MediaConnectGatewayInstanceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `MediaConnectGatewayInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 22. März 2023, 20:43 UTC
- Bearbeitete Zeit: 22. März 2023, 20:43 UTC
- ARN: `arn:aws:iam::aws:policy/MediaConnectGatewayInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
```

```
  "Statement" : [
    {
      "Sid" : "MediaConnectGateway",
      "Effect" : "Allow",
      "Action" : [
        "mediaconnect:DiscoverGatewayPollEndpoint",
        "mediaconnect:PollGateway",
        "mediaconnect:SubmitGatewayStateChange"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MediaPackageServiceRolePolicy

Beschreibung: Ermöglicht das MediaPackage Veröffentlichen von Protokollen in CloudWatch

`MediaPackageServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. September 2020, 17:45 Uhr UTC
- Bearbeitete Zeit: 18. September 2020, 17:45 UTC

- ARN: `arn:aws:iam::aws:policy/aws-service-role/MediaPackageServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "logs:PutLogEvents",
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*:log-stream:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/MediaPackage/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MemoryDBServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht es MemoryDB, AWS Ressourcen in Ihrem Namen zu verwalten, soweit dies für die Verwaltung Ihrer Ressourcen erforderlich ist.

`MemoryDBServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 17. August 2021, 22:34 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 16:21 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MemoryDBServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CreateMemoryDBTagsOnNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonMemoryDBManaged"
          ]
        }
      }
    },
    {
      "Sid" : "CreateNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "DeleteMemoryDBTaggedNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/AmazonMemoryDBManaged" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteNetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
```

```
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*"
    },
    {
      "Sid" : "DescribeEC2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PutCloudWatchMetricData",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/MemoryDB"
        }
      }
    },
    {
      "Sid" : "ReplicateMemoryDBMultiRegionClusterData",
      "Effect" : "Allow",
      "Action" : [
        "memorydb:ReplicateMultiRegionClusterData"
      ],
      "Resource" : "arn:aws:memorydb:*:*:cluster/*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubDMSAccessServiceRolePolicy

Beschreibung: Richtlinie für den Database Migration Service, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`MigrationHubDMSAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 17:50 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 17:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubDMSAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
```

```
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/DMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubServiceRolePolicy

Beschreibung: Ermöglicht Migration Hub, den Application Discovery Service in Ihrem Namen aufzurufen

`MigrationHubServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 17:22 Uhr UTC
- Bearbeitete Zeit: 6. August 2020, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "discovery:ListConfigurations",
```

```
        "discovery:DescribeConfigurations"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "dms:AddTagsToResource",
      "Resource" : [
        "arn:aws:dms:*:*:endpoint:*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "aws:migrationhub:source-id"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceAttribute"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MigrationHubSMSAccessServiceRolePolicy

Beschreibung: Richtlinie für den Servermigrationsdienst, die Rolle im Kundenkonto zu übernehmen, um Migration Hub anzurufen

`MigrationHubSMSAccessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. Juni 2019, 18:30 Uhr UTC
- Bearbeitete Zeit: 7. Oktober 2019, 18:02 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MigrationHubSMSAccessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "mgh:CreateProgressUpdateStream",
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:DescribeMigrationTask",
        "mgh:AssociateDiscoveredResource",
        "mgh:ListDiscoveredResources",
        "mgh:ImportMigrationTask",
        "mgh:ListCreatedArtifacts",
        "mgh:DisassociateDiscoveredResource",
        "mgh:AssociateCreatedArtifact",
        "mgh:NotifyMigrationTaskState",
        "mgh:DisassociateCreatedArtifact",
        "mgh:PutResourceAttributes"
      ],
      "Resource" : "arn:aws:mgh:*:*:progressUpdateStream/SMS/migrationTask/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "mgh:ListMigrationTasks",
        "mgh:NotifyApplicationState",
        "mgh:DescribeApplicationState",
        "mgh:GetHomeRegion"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MonitronServiceRolePolicy

Beschreibung: Richtlinie für die serviceverknüpfte Rolle von AWS Monitron, die Zugriff auf die erforderlichen Kundenressourcen gewährt.

`MonitronServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 2. Mai 2022, 19:22 UTC
- Bearbeitete Zeit: 2. Mai 2022, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/MonitronServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/monitron/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MultiPartyApprovalFullAccess

Beschreibung: Bietet vollen Zugriff auf die Genehmigung durch mehrere Parteien. Diese Richtlinie umfasst auch entsprechende Berechtigungen für AWS Organizations und AWS IAM Identity zur Verwaltung von Genehmigungsteams und Identitätsquellen.

`MultiPartyApprovalFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `MultiPartyApprovalFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2025, 20:22 UTC
- Bearbeitete Zeit: 8. September 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaFullAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOCreateApplication",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication"
      ],
      "Resource" : [
        "arn:aws:sso:::instance/*",
        "arn:aws:sso::aws:applicationProvider/mpa"
      ]
    },
    {
```

```
      "Sid" : "SSOApplicationManagement",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication",
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationGrant",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationAccessScope",
        "sso:DeleteApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "mpa.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "sso:ListInstances"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
 "arn:*:identitystore::*:identitystore/*"
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

MultiPartyApprovalReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Genehmigungen durch mehrere Parteien. Diese Richtlinie umfasst auch die entsprechenden Leseberechtigungen für AWS Organizations und AWS IAM Identity für Genehmigungsteams und Identitätsquellen.

`MultiPartyApprovalReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `MultiPartyApprovalReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. Juni 2025, 20:07 UTC
- Bearbeitete Zeit: 8. September 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/MultiPartyApprovalReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "MpaReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "mpa:Get*",
        "mpa:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators",
```

```
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSOManagementAccess",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:DescribeRegisteredRegions",
        "sso:GetSharedSsoConfiguration",
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityCenter",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:sso:instance-arn" : "arn:*:sso:::instance/*"
        },
        "StringLike" : {
          "kms:ViaService" : "sso.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowKmsAccessViaIdentityStore",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "kms:EncryptionContext:aws:identitystore:identitystore-arn" :
"arn:*:identitystore::*:identitystore/*"
```

```
        },
        "StringLike" : {
          "kms:ViaService" : "identitystore.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf die Verwaltung von Amazon Neptune mithilfe der. AWS-Managementkonsole Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos, Berechtigungen zum Erstellen und Bearbeiten von EC2 Amazon-Instances und VPC-Konfigurationen, Berechtigungen zum Anzeigen und Auflisten von Schlüsseln in Amazon KMS sowie vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter FAQs/. https://aws.amazon.com/neptune/

`NeptuneConsoleFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `NeptuneConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. Juni 2018, 21:35 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
```

```
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
```

```
        "rds:ModifyEventSubscription",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:RestoreDBClusterToPointInTime"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeAccountAttributes",
```

```
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcs",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Action" : "iam:PassRole",
      "Effect" : "Allow",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Action" : "iam:CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:GetGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:UpdateGraph",
        "neptune-graph:ResetGraph",
        "neptune-graph:CreateGraphSnapshot",
        "neptune-graph:DeleteGraphSnapshot",
        "neptune-graph:GetGraphSnapshot",
        "neptune-graph:ListGraphSnapshots",
        "neptune-graph:RestoreGraphFromSnapshot",
        "neptune-graph:CreatePrivateGraphEndpoint",
        "neptune-graph:GetPrivateGraphEndpoint",
        "neptune-graph:ListPrivateGraphEndpoints",
        "neptune-graph:DeletePrivateGraphEndpoint",
        "neptune-graph:CreateGraphUsingImportTask",
        "neptune-graph:GetImportTask",
        "neptune-graph:ListImportTasks",
        "neptune-graph:CancelImportTask"
      ],
      "Resource" : [
```

```
        "arn:aws:neptune-graph:*:*:*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "neptune-graph.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowCreateSLRForNeptuneAnalytics",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "neptune-graph.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Neptune. Beachten Sie, dass diese Richtlinie auch vollen Zugriff auf Veröffentlichungen zu allen SNS-Themen innerhalb des Kontos sowie vollen Zugriff auf Amazon RDS gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/FAQs/.

`NeptuneFullAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `NeptuneFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2018, 19:17 UTC
- Bearbeitete Zeit: 22. Januar 2024, 16:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneFullAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowNeptuneCreate",
      "Effect" : "Allow",
      "Action" : [
        "rds:CreateDBCluster",
```

```
        "rds:CreateDBInstance"
      ],
      "Resource" : [
        "arn:aws:rds:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "rds:DatabaseEngine" : [
            "graphdb",
            "neptune"
          ]
        }
      }
    },
    {
      "Sid" : "AllowManagementPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:AddRoleToDBCluster",
        "rds:AddSourceIdentifierToSubscription",
        "rds:AddTagsToResource",
        "rds:ApplyPendingMaintenanceAction",
        "rds:CopyDBClusterParameterGroup",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBParameterGroup",
        "rds:CreateDBClusterEndpoint",
        "rds:CreateDBClusterParameterGroup",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBParameterGroup",
        "rds:CreateDBSubnetGroup",
        "rds:CreateEventSubscription",
        "rds:CreateGlobalCluster",
        "rds:DeleteDBCluster",
        "rds:DeleteDBClusterEndpoint",
        "rds:DeleteDBClusterParameterGroup",
        "rds:DeleteDBClusterSnapshot",
        "rds:DeleteDBInstance",
        "rds:DeleteDBParameterGroup",
        "rds:DeleteDBSubnetGroup",
        "rds:DeleteEventSubscription",
        "rds:DeleteGlobalCluster",
        "rds:DescribeDBClusterEndpoints",
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
```

```
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSecurityGroups",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEngineDefaultClusterParameters",
        "rds:DescribeEngineDefaultParameters",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DescribeValidDBInstanceModifications",
        "rds:DownloadDBLogFilePortion",
        "rds:FailoverDBCluster",
        "rds:FailoverGlobalCluster",
        "rds:ListTagsForResource",
        "rds:ModifyDBCluster",
        "rds:ModifyDBClusterEndpoint",
        "rds:ModifyDBClusterParameterGroup",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBInstance",
        "rds:ModifyDBParameterGroup",
        "rds:ModifyDBSubnetGroup",
        "rds:ModifyEventSubscription",
        "rds:ModifyGlobalCluster",
        "rds:PromoteReadReplicaDBCluster",
        "rds:RebootDBInstance",
        "rds:RemoveFromGlobalCluster",
        "rds:RemoveRoleFromDBCluster",
        "rds:RemoveSourceIdentifierFromSubscription",
        "rds:RemoveTagsFromResource",
        "rds:ResetDBClusterParameterGroup",
        "rds:ResetDBParameterGroup",
        "rds:RestoreDBClusterFromSnapshot",
```

```
        "rds:RestoreDBClusterToPointInTime",
        "rds:StartDBCluster",
        "rds:StopDBCluster"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowOtherDepedentPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "kms:ListAliases",
        "kms:ListKeyPolicies",
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "sns:ListSubscriptions",
        "sns:ListTopics",
        "sns:Publish"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowPassRoleForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "rds.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "AllowCreateSLRForNeptune",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "rds.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowDataAccessForNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:*"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneGraphReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf alle Amazon Neptune Analytics-Ressourcen sowie Nur-Lese-Berechtigungen für abhängige Dienste.

`NeptuneGraphReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `NeptuneGraphReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. November 2023, 07:32 UTC
- Bearbeitete Zeit: 30. November 2023, 07:32 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneGraphReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneGraph",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:Get*",
        "neptune-graph:List*",
        "neptune-graph:Read*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
```

```
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NeptuneReadOnlyAccess

Beschreibung: Bietet Lesezugriff auf Amazon Neptune. Beachten Sie, dass diese Richtlinie auch Zugriff auf Amazon RDS-Ressourcen gewährt. Weitere Informationen finden Sie unter https://aws.amazon.com/neptune/ FAQs/.

`NeptuneReadOnlyAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `NeptuneReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. Mai 2018, 19:16 UTC
- Bearbeitete Zeit: 22. Januar 2024, 16:33 UTC
- ARN: `arn:aws:iam::aws:policy/NeptuneReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowReadOnlyPermissionsForRDS",
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeAccountAttributes",
        "rds:DescribeCertificates",
        "rds:DescribeDBClusterParameterGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBClusterSnapshotAttributes",
        "rds:DescribeDBClusterSnapshots",
        "rds:DescribeDBClusters",
        "rds:DescribeDBEngineVersions",
        "rds:DescribeDBInstances",
        "rds:DescribeDBLogFiles",
        "rds:DescribeDBParameterGroups",
        "rds:DescribeDBParameters",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeEventCategories",
        "rds:DescribeEventSubscriptions",
        "rds:DescribeEvents",
        "rds:DescribeGlobalClusters",
        "rds:DescribeOrderableDBInstanceOptions",
        "rds:DescribePendingMaintenanceActions",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForCloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "AllowReadOnlyPermissionsForEC2",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListKeys",
        "kms:ListRetirableGrants",
        "kms:ListAliases",
        "kms:ListKeyPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/rds/*:log-stream:*",
        "arn:aws:logs:*:*:log-group:/aws/neptune/*:log-stream:*"
      ]
    },
    {
      "Sid" : "AllowReadOnlyPermissionsForNeptuneDB",
      "Effect" : "Allow",
      "Action" : [
        "neptune-db:Read*",
        "neptune-db:Get*",
        "neptune-db:List*"
      ],
```

```
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NetworkAdministrator

Beschreibung: Gewährt vollständige Zugriffsberechtigungen für AWS Dienste und Aktionen, die für die Einrichtung und Konfiguration von AWS Netzwerkressourcen erforderlich sind.

`NetworkAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `NetworkAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:31 Uhr UTC
- Bearbeitete Zeit: 19. Dezember 2024, 22:52 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/NetworkAdministrator`

Version der Richtlinie

Richtlinienversion: v13 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowDefaultNetworkAdminActions",
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:Describe*",
        "cloudfront:ListDistributions",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "directconnect:*",
        "ec2:AcceptVpcEndpointConnections",
        "ec2:AllocateAddress",
        "ec2:AssignIpv6Addresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:AssociateAddress",
        "ec2:AssociateDhcpOptions",
        "ec2:AssociateRouteTable",
        "ec2:AssociateSubnetCidrBlock",
        "ec2:AssociateVpcCidrBlock",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:CreateCarrierGateway",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDefaultSubnet",
        "ec2:CreateDefaultVpc",
        "ec2:CreateDhcpOptions",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateFlowLogs",
        "ec2:CreateInternetGateway",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkAcl",
```

```
        "ec2:CreateNetworkAclEntry",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpcEndpointConnectionNotification",
        "ec2:CreateVpcEndpointServiceConfiguration",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteCarrierGateway",
        "ec2:DeleteEgressOnlyInternetGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpointConnectionNotifications",
        "ec2:DeleteVpcEndpointServiceConfigurations",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeIpv6Pools",
```

```
        "ec2:DescribeKeyPairs",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribePublicIpv4Pools",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:DisassociateSubnetCidrBlock",
        "ec2:DisassociateVpcCidrBlock",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetVpnConnectionDeviceSampleConfiguration",
        "ec2:GetVpnConnectionDeviceTypes",
        "ec2:GetVpnTunnelReplacementStatus",
```

```
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:ModifySecurityGroupRules",
        "ec2:ModifySubnetAttribute",
        "ec2:ModifyVpcAttribute",
        "ec2:ModifyVpcEndpoint",
        "ec2:ModifyVpcEndpointConnectionNotification",
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:ModifyVpcEndpointServicePermissions",
        "ec2:ModifyVpcPeeringConnectionOptions",
        "ec2:ModifyVpcTenancy",
        "ec2:ModifyVpnConnection",
        "ec2:ModifyVpnConnectionOptions",
        "ec2:ModifyVpnTunnelCertificate",
        "ec2:ModifyVpnTunnelOptions",
        "ec2:MoveAddressToVpc",
        "ec2:RejectVpcEndpointConnections",
        "ec2:ReleaseAddress",
        "ec2:ReplaceNetworkAclAssociation",
        "ec2:ReplaceNetworkAclEntry",
        "ec2:ReplaceRoute",
        "ec2:ReplaceRouteTableAssociation",
        "ec2:ReplaceVpnTunnel",
        "ec2:ResetNetworkInterfaceAttribute",
        "ec2:RestoreAddressToClassic",
        "ec2:UnassignIpv6Addresses",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticloadbalancing:*",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "route53:*",
        "route53domains:*",
        "sns:CreateTopic",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowVPCPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AssociateSecurityGroupVpc",
        "ec2:AttachClassicLinkVpc",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl",
        "ec2:DeleteNetworkAclEntry",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DescribeSecurityGroupVpcAssociations",
        "ec2:DetachClassicLinkVpc",
        "ec2:DisableVpcClassicLink",
        "ec2:DisassociateSecurityGroupVpc",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "AllowLocalGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateLocalGatewayRoute",
        "ec2:CreateLocalGatewayRouteTableVpcAssociation",
        "ec2:DeleteLocalGatewayRoute",
        "ec2:DeleteLocalGatewayRouteTableVpcAssociation",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
```

```
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeLocalGateways",
        "ec2:SearchLocalGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DiscoverBuckets",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation",
        "s3:GetBucketWebsite",
        "s3:ListBucket"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DiscoverFlowLogRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/flow-logs-*"
    },
    {
      "Sid" : "NetworkmanagerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "networkmanager:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TransitGatewayPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AcceptTransitGatewayVpcAttachment",
```

```
        "ec2:AssociateTransitGatewayRouteTable",
        "ec2:CreateTransitGateway",
        "ec2:CreateTransitGatewayRoute",
        "ec2:CreateTransitGatewayRouteTable",
        "ec2:CreateTransitGatewayVpcAttachment",
        "ec2:DeleteTransitGateway",
        "ec2:DeleteTransitGatewayRoute",
        "ec2:DeleteTransitGatewayRouteTable",
        "ec2:DeleteTransitGatewayVpcAttachment",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DisableTransitGatewayRouteTablePropagation",
        "ec2:DisassociateTransitGatewayRouteTable",
        "ec2:EnableTransitGatewayRouteTablePropagation",
        "ec2:ExportTransitGatewayRoutes",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:ModifyTransitGateway",
        "ec2:ModifyTransitGatewayVpcAttachment",
        "ec2:RejectTransitGatewayVpcAttachment",
        "ec2:ReplaceTransitGatewayRoute",
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowTransitGatewaySLRCreation",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : [
            "transitgateway.amazonaws.com"
          ]
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NetworkSecurityDirectorServiceLinkedRolePolicy

Beschreibung: Stellt Berechtigungen für die dienstverknüpfte Rolle AWS Shield Network Security Director bereit, um bestimmte Umgebungen zu bewerten.

`NetworkSecurityDirectorServiceLinkedRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 13. Juni 2025, 20:07 UTC
- Bearbeitete Zeit: 10. November 2025, 19:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NetworkSecurityDirectorServiceLinkedRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ResourceLevelPermissionNotSupported",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayAttachments",
        "ec2:DescribeTransitGatewayPeeringAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:GetManagedPrefixListEntries",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTags",
```

```
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "wafv2:ListWebACLs",
        "cloudfront:ListDistributions",
        "cloudfront:ListTagsForResource",
        "directconnect:DescribeDirectConnectGateways",
        "directconnect:DescribeVirtualInterfaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "cloudfront",
      "Effect" : "Allow",
      "Action" : [
        "cloudfront:GetDistribution"
      ],
      "Resource" : "arn:aws:cloudfront::*:distribution/*"
    },
    {
      "Sid" : "classicWaf",
      "Effect" : "Allow",
      "Action" : [
        "waf:ListWebACLs",
        "waf:GetWebACL"
      ],
      "Resource" : [
        "arn:aws:waf::*:webacl/*",
        "arn:aws:waf-regional:*:*:webacl/*"
      ]
    },
    {
      "Sid" : "wafv2",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:GetRuleGroup",
        "wafv2:DescribeManagedRuleGroup",
        "wafv2:GetWebACL"
      ],
```

```
      "Resource" : [
        "arn:aws:wafv2:*:*:global/rulegroup/*",
        "arn:aws:wafv2:*:*:regional/rulegroup/*",
        "arn:aws:wafv2:*:*:global/managedruleset/*",
        "arn:aws:wafv2:*:*:regional/managedruleset/*",
        "arn:aws:wafv2:*:*:global/webacl/*/*",
        "arn:aws:wafv2:*:*:regional/webacl/*/*",
        "arn:aws:apprunner:*:*:service/*",
        "arn:aws:cognito-idp:*:*:userpool/*",
        "arn:aws:ec2:*:*:verified-access-instance/*"
      ]
    },
    {
      "Sid" : "directconnect",
      "Effect" : "Allow",
      "Action" : [
        "directconnect:DescribeConnections",
        "directconnect:DescribeDirectConnectGatewayAssociations",
        "directconnect:DescribeDirectConnectGatewayAttachments",
        "directconnect:DescribeVirtualGateways"
      ],
      "Resource" : [
        "arn:aws:directconnect::*:dx-gateway/*",
        "arn:aws:directconnect:*:*:dxcon/*",
        "arn:aws:directconnect:*:*:dxlag/*",
        "arn:aws:directconnect:*:*:dxvif/*"
      ]
    },
    {
      "Sid" : "ec2Get",
      "Effect" : "Allow",
      "Action" : [
        "ec2:SearchTransitGatewayRoutes"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:transit-gateway-route-table/*"
      ]
    },
    {
      "Sid" : "networkFirewall",
      "Effect" : "Allow",
      "Action" : [
        "network-firewall:ListFirewalls",
        "network-firewall:ListFirewallPolicies",
```

```
        "network-firewall:ListRuleGroups",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeRuleGroup"
      ],
      "Resource" : [
        "arn:aws:network-firewall:*:*:*/*"
      ]
    },
    {
      "Sid" : "apiGatewayGetAPI",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*",
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks",
        "arn:aws:apigateway:*::/vpclinks/*"
      ]
    },
    {
      "Sid" : "AllowOrganizationsReadAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListTargetsForPolicy"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "AllowOrganizationsAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "organizations:ServicePrincipal" : [
            "network-security-director.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowAccountInformationRead",
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetRegionOptStatus"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderList",
      "Effect" : "Allow",
      "Action" : [
        "config:ListConfigurationRecorders"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowConfigRecorderScopedAccess",
      "Effect" : "Allow",
      "Action" : [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:PutServiceLinkedConfigurationRecorder",
        "config:DeleteServiceLinkedConfigurationRecorder"
      ],
      "Condition" : {
        "StringLikeIfExists" : {
          "config:ConfigurationRecorderServicePrincipal" : [
```

```
            "network-security-director.amazonaws.com"
          ]
        }
      },
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

NovaActServiceRolePolicy

Beschreibung: Diese Richtlinie ermöglicht NovaAct die Erstellung und Verwaltung der für den Betrieb der Nova Act-Agenten erforderlichen Ressourcen.

`NovaActServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. November 2025, 16:19 UTC
- Bearbeitete Zeit: 26. November 2025, 16:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/NovaActServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowPublishCloudWatchMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/NovaAct"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OAMFullAccess

Beschreibung: Bietet vollen Zugriff auf CloudWatch Observability Access Manager

`OAMFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `OAMFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:38 UTC
- Zeit bearbeitet: 27. November 2022, 13:38 UTC
- ARN: `arn:aws:iam::aws:policy/OAMFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "oam:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center

- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OAMReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf CloudWatch Observability Access Manager

`OAMReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `OAMReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2022, 13:29 UTC
- Zeit bearbeitet: 27. November 2022, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/OAMReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Effect" : "Allow",
      "Action" : [
        "oam:Get*",
        "oam:List*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

OpensearchIngestionSelfManagedVpcePolicy

Beschreibung: Ermöglicht Amazon OpenSearch Ingestion, Netzwerkressourcen zu beschreiben und Servicemetriken in Cloudwatch zu schreiben

`OpensearchIngestionSelfManagedVpcePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 10. Juni 2024, 19:59 UTC
- Bearbeitete Zeit: 10. Juni 2024, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/OpensearchIngestionSelfManagedVpcePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CwPermissionsForOsiNamespace",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/OSIS"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

PartnerCentralAccountManagementUserRoleAssociation

Beschreibung: Ermöglicht das Zuordnen und Trennen von Partnern Central-Benutzern zu IAM-Rollen

`PartnerCentralAccountManagementUserRoleAssociation`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `PartnerCentralAccountManagementUserRoleAssociation` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 10. November 2023, 02:03 UTC
- Bearbeitete Zeit: 10. November 2023, 02:03 UTC
- ARN: `arn:aws:iam::aws:policy/PartnerCentralAccountManagementUserRoleAssociation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "PassPartnerCentralRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/PartnerCentralRoleFor*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "partnercentral-account-management.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PartnerUserRoleAssociation",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "partnercentral-account-management:AssociatePartnerUser",
        "partnercentral-account-management:DisassociatePartnerUser"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

PowerUserAccess

Beschreibung: Bietet vollen Zugriff auf AWS Dienste und Ressourcen, ermöglicht jedoch keine Verwaltung von Benutzern und Gruppen.

`PowerUserAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `PowerUserAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 29. April 2025, 19:07 UTC
- ARN: `arn:aws:iam::aws:policy/PowerUserAccess`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "NotAction" : [
        "iam:*",
        "organizations:*",
        "account:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "account:GetAccountInformation",
        "account:GetPrimaryEmail",
        "account:ListRegions",
```

```
        "iam:CreateServiceLinkedRole",
        "iam:DeleteServiceLinkedRole",
        "iam:ListRoles",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QAppsServiceRolePolicy

Beschreibung: Erteilt Berechtigungen für AWS-Services und Ressourcen, die von Amazon Q Apps verwendet oder verwaltet werden.

`QAppsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 26. September 2024, 19:22 UTC
- Bearbeitete Zeit: 26. September 2024, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QAppsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QAppsPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QApps"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QBusinessQuicksightPluginPolicy

Beschreibung: Erteilt die Erlaubnis QBusiness , das QuickSight Plugin aufzurufen QuickSight APIs

`QBusinessQuicksightPluginPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `QBusinessQuicksightPluginPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 03. Dezember 2024, 15:36 UTC
- Bearbeitete Zeit: 3. Dezember 2024, 15:36 UTC
- ARN: `arn:aws:iam::aws:policy/QBusinessQuicksightPluginPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessToQuickSightPredictQAResultsInvocation",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PredictQAResults"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:topic/*",
        "arn:aws:quicksight:*:*:dashboard/*"
      ]
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QBusinessServiceRolePolicy

Beschreibung: Erteilt Berechtigungen für AWS-Services und Ressourcen, die von Amazon Q verwendet oder verwaltet werden

`QBusinessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. April 2024, 16:05 UTC
- Bearbeitete Zeit: 29. April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/QBusinessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "QBusinessPutMetricDataPermission",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/QBusiness"
        }
      }
    },
    {
      "Sid" : "QBusinessCreateLogGroupPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessDescribeLogGroupsPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QBusinessLogStreamPermission",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/qbusiness/*:log-stream:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

QuickSightAccessForS3StorageManagementAnalyticsReadOnly

Beschreibung: Richtlinie, die vom QuickSight Team für den Zugriff auf Kundendaten verwendet wird, die von S3 Storage Management Analytics erstellt wurden.

`QuickSightAccessForS3StorageManagementAnalyticsReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `QuickSightAccessForS3StorageManagementAnalyticsReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 12. Juni 2017, 18:18 Uhr UTC
- Bearbeitete Zeit: 8. Oktober 2019, 23:53 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/QuickSightAccessForS3StorageManagementAnalyticsReadOnly`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::s3-analytics-export-shared-*"
      ]
    },
    {
      "Action" : [
        "s3:GetAnalyticsConfiguration",
```

```
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

RDSCloudHsmAuthorizationRole

Beschreibung: Standardrichtlinie für die Amazon RDS-Servicerolle.

`RDSCloudHsmAuthorizationRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `RDSCloudHsmAuthorizationRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Bearbeitete Zeit: 26. September 2019, 22:14 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/RDSCloudHsmAuthorizationRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudhsm:CreateLunaClient",
        "cloudhsm:DeleteLunaClient",
        "cloudhsm:DescribeHapg",
        "cloudhsm:DescribeLunaClient",
        "cloudhsm:GetConfig",
        "cloudhsm:ModifyHapg",
        "cloudhsm:ModifyLunaClient"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf AWS Dienste und Ressourcen.

`ReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 16. Dezember 2025, 13:04 UTC
- ARN: `arn:aws:iam::aws:policy/ReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v137 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadOnlyActionsGroup1",
      "Effect" : "Allow",
      "Action" : [
        "a4b:Get*",
        "a4b:List*",
        "a4b:Search*",
        "access-analyzer:GetAccessPreview",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:GetFindingsStatistics",
        "access-analyzer:GetGeneratedPolicy",
        "access-analyzer:ListAccessPreviewFindings",
```

```
        "access-analyzer:ListAccessPreviews",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListPolicyGenerations",
        "access-analyzer:ListTagsForResource",
        "access-analyzer:ValidatePolicy",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetContactInformation",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "account:ListRegions",
        "acm-pca:Describe*",
        "acm-pca:Get*",
        "acm-pca:List*",
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "action-recommendations:ListRecommendedActions",
        "aiops:GetEphemeralInvestigationResults",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationEvent",
        "aiops:GetInvestigationGroup",
        "aiops:GetInvestigationResource",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "aiops:ValidateInvestigationGroup",
        "aiops:GetFact",
        "aiops:GetFactVersions",
        "aiops:GetReport",
        "aiops:ListFacts",
        "airflow:ListEnvironments",
        "airflow:ListTagsForResource",
        "amplify:GetApp",
        "amplify:GetBackendEnvironment",
        "amplify:GetBranch",
        "amplify:GetDomainAssociation",
        "amplify:GetJob",
        "amplify:GetWebhook",
        "amplify:ListApps",
        "amplify:ListArtifacts",
```

```
        "amplify:ListBackendEnvironments",
        "amplify:ListBranches",
        "amplify:ListDomainAssociations",
        "amplify:ListJobs",
        "amplify:ListTagsForResource",
        "amplify:ListWebhooks",
        "aoss:BatchGetCollection",
        "aoss:BatchGetLifecyclePolicy",
        "aoss:BatchGetVpcEndpoint",
        "aoss:GetAccessPolicy",
        "aoss:GetAccountSettings",
        "aoss:GetPoliciesStats",
        "aoss:GetSecurityConfig",
        "aoss:GetSecurityPolicy",
        "aoss:ListAccessPolicies",
        "aoss:ListCollections",
        "aoss:ListLifecyclePolicies",
        "aoss:ListSecurityConfigs",
        "aoss:ListSecurityPolicies",
        "aoss:ListTagsForResource",
        "aoss:ListVpcEndpoints",
        "apigateway:GET",
        "appconfig:GetApplication",
        "appconfig:GetConfiguration",
        "appconfig:GetConfigurationProfile",
        "appconfig:GetDeployment",
        "appconfig:GetDeploymentStrategy",
        "appconfig:GetEnvironment",
        "appconfig:GetExtension",
        "appconfig:GetHostedConfigurationVersion",
        "appconfig:ListApplications",
        "appconfig:ListConfigurationProfiles",
        "appconfig:ListDeploymentStrategies",
        "appconfig:ListDeployments",
        "appconfig:ListEnvironments",
        "appconfig:ListExtensions",
        "appconfig:ListHostedConfigurationVersions",
        "appconfig:ListTagsForResource",
        "appfabric:GetAppAuthorization",
        "appfabric:GetAppBundle",
        "appfabric:GetIngestion",
        "appfabric:GetIngestionDestination",
        "appfabric:ListAppAuthorizations",
        "appfabric:ListAppBundles",
```

```
        "appfabric:ListIngestionDestinations",
        "appfabric:ListIngestions",
        "appfabric:ListTagsForResource",
        "appflow:DescribeConnector",
        "appflow:DescribeConnectorEntity",
        "appflow:DescribeConnectorFields",
        "appflow:DescribeConnectorProfiles",
        "appflow:DescribeConnectors",
        "appflow:DescribeFlow",
        "appflow:DescribeFlowExecution",
        "appflow:DescribeFlowExecutionRecords",
        "appflow:DescribeFlows",
        "appflow:ListConnectorEntities",
        "appflow:ListConnectorFields",
        "appflow:ListConnectors",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "application-autoscaling:GetPredictiveScalingForecast",
        "application-autoscaling:ListTagsForResource",
        "application-signals:BatchGetServiceLevelObjectiveBudgetReport",
        "application-signals:GetService",
        "application-signals:GetServiceLevelObjective",
        "application-signals:ListObservedEntities",
        "application-signals:ListServiceDependencies",
        "application-signals:ListServiceDependents",
        "application-signals:ListServiceLevelObjectives",
        "application-signals:ListServiceOperations",
        "application-signals:ListServices",
        "application-signals:ListTagsForResource",
        "application-signals:ListServiceStates",
        "application-signals:ListAuditFindings",
        "application-signals:ListGroupingAttributeDefinitions",
        "application-signals:ListServiceLevelObjectiveExclusionWindows",
        "application-signals:ListEntityEvents",
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
```

```
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListServicesForAutoScalingConfiguration",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
        "appstream:Describe*",
        "appstream:List*",
        "appstudio:GetAccountStatus",
        "appstudio:GetEnablementJobStatus",
        "appsync:Get*",
        "appsync:List*",
        "apptest:GetTestCase",
        "apptest:GetTestConfiguration",
        "apptest:GetTestRunStep",
        "apptest:GetTestSuite",
        "apptest:ListTagsForResource",
        "apptest:ListTestCases",
        "apptest:ListTestConfigurations",
        "apptest:ListTestRunSteps",
        "apptest:ListTestRunTestCases",
        "apptest:ListTestRuns",
        "apptest:ListTestSuites",
        "aps:DescribeAlertManagerDefinition",
        "aps:DescribeLoggingConfiguration",
        "aps:DescribeRuleGroupsNamespace",
        "aps:DescribeScraper",
        "aps:DescribeWorkspace",
        "aps:GetAlertManagerSilence",
        "aps:GetAlertManagerStatus",
        "aps:GetDefaultScraperConfiguration",
        "aps:GetLabels",
        "aps:GetMetricMetadata",
        "aps:GetSeries",
        "aps:ListAlertManagerAlertGroups",
        "aps:ListAlertManagerAlerts",
        "aps:ListAlertManagerReceivers",
        "aps:ListAlertManagerSilences",
```

```
        "aps:ListAlerts",
        "aps:ListRuleGroupsNamespaces",
        "aps:ListRules",
        "aps:ListScrapers",
        "aps:ListTagsForResource",
        "aps:ListWorkspaces",
        "aps:QueryMetrics",
        "arc-region-switch:GetPlan",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlans",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListTagsForResource",
        "arc-zonal-shift:GetAutoshiftObserverNotificationStatus",
        "arc-zonal-shift:GetManagedResource",
        "arc-zonal-shift:ListAutoshifts",
        "arc-zonal-shift:ListManagedResources",
        "arc-zonal-shift:ListZonalShifts",
        "artifact:GetCustomerAgreement",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements",
        "artifact:ListReports",
        "athena:Batch*",
        "athena:Get*",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:GetAssessment",
        "auditmanager:GetAssessmentFramework",
        "auditmanager:GetAssessmentReportUrl",
        "auditmanager:GetChangeLogs",
        "auditmanager:GetControl",
        "auditmanager:GetDelegations",
        "auditmanager:GetEvidence",
        "auditmanager:GetEvidenceByEvidenceFolder",
        "auditmanager:GetEvidenceFolder",
        "auditmanager:GetEvidenceFoldersByAssessment",
        "auditmanager:GetEvidenceFoldersByAssessmentControl",
```

```
        "auditmanager:GetOrganizationAdminAccount",
        "auditmanager:GetServicesInScope",
        "auditmanager:GetSettings",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControls",
        "auditmanager:ListKeywordsForDataSource",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "auditmanager:ValidateAssessmentReportIntegrity",
        "autoscaling-plans:Describe*",
        "autoscaling-plans:GetScalingPlanResourceForecastData",
        "autoscaling:Describe*",
        "autoscaling:GetPredictiveScalingForecast",
        "aws-portal:View*",
        "backup-gateway:GetBandwidthRateLimitSchedule",
        "backup-gateway:GetGateway",
        "backup-gateway:GetHypervisor",
        "backup-gateway:GetHypervisorPropertyMappings",
        "backup-gateway:GetVirtualMachine",
        "backup-gateway:ListGateways",
        "backup-gateway:ListHypervisors",
        "backup-gateway:ListTagsForResource",
        "backup-gateway:ListVirtualMachines",
        "backup:Describe*",
        "backup:Get*",
        "backup:List*",
        "batch:Describe*",
        "batch:List*",
        "bedrock-agentcore:GetAgentRuntime",
        "bedrock-agentcore:GetAgentRuntimeEndpoint",
        "bedrock-agentcore:GetApiKeyCredentialProvider",
        "bedrock-agentcore:GetBrowser",
        "bedrock-agentcore:GetBrowserSession",
        "bedrock-agentcore:GetCodeInterpreter",
        "bedrock-agentcore:GetCodeInterpreterSession",
        "bedrock-agentcore:GetEvent",
        "bedrock-agentcore:GetGateway",
        "bedrock-agentcore:GetGatewayTarget",
        "bedrock-agentcore:GetMemory",
        "bedrock-agentcore:GetMemoryRecord",
        "bedrock-agentcore:GetOauth2CredentialProvider",
        "bedrock-agentcore:GetTokenVault",
```

```
        "bedrock-agentcore:GetWorkloadIdentity",
        "bedrock-agentcore:ListAgentRuntimeEndpoints",
        "bedrock-agentcore:ListAgentRuntimes",
        "bedrock-agentcore:ListAgentRuntimeVersions",
        "bedrock-agentcore:ListApiKeyCredentialProviders",
        "bedrock-agentcore:ListBrowsers",
        "bedrock-agentcore:ListBrowserSessions",
        "bedrock-agentcore:ListCodeInterpreters",
        "bedrock-agentcore:ListCodeInterpreterSessions",
        "bedrock-agentcore:ListEvents",
        "bedrock-agentcore:ListGateways",
        "bedrock-agentcore:ListGatewayTargets",
        "bedrock-agentcore:ListMemories",
        "bedrock-agentcore:ListMemoryRecords",
        "bedrock-agentcore:ListOauth2CredentialProviders",
        "bedrock-agentcore:ListWorkloadIdentities",
        "bedrock-agentcore:RetrieveMemoryRecords",
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentCollaborator",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:GetCustomModel",
        "bedrock:GetDataSource",
        "bedrock:GetEvaluationJob",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:GetFlowVersion",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetGuardrail",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelInvocationJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPrompt",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentCollaborators",
```

```
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListAgents",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlowVersions",
        "bedrock:ListFlows",
        "bedrock:ListFoundationModelAgreementOffers",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetBillingView",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetResourcePolicy",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "billing:ListSourceViewsForBillingView",
        "billing:ListTagsForResource",
        "billingconductor:GetBillingGroupCostReport",
        "billingconductor:ListAccountAssociations",
        "billingconductor:ListBillingGroupCostReports",
        "billingconductor:ListBillingGroups",
        "billingconductor:ListCustomLineItemVersions",
        "billingconductor:ListCustomLineItems",
        "billingconductor:ListPricingPlans",
        "billingconductor:ListPricingPlansAssociatedWithPricingRule",
        "billingconductor:ListPricingRules",
        "billingconductor:ListPricingRulesAssociatedToPricingPlan",
        "billingconductor:ListResourcesAssociatedToCustomLineItem",
        "billingconductor:ListTagsForResource",
```

```
        "braket:GetDevice",
        "braket:GetJob",
        "braket:GetQuantumTask",
        "braket:SearchDevices",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "budgets:Describe*",
        "budgets:ListTagsForResource",
        "budgets:View*",
        "cassandra:Select",
        "ce:DescribeCostCategoryDefinition",
        "ce:DescribeNotificationSubscription",
        "ce:DescribeReport",
        "ce:GetAnomalies",
        "ce:GetAnomalyMonitors",
        "ce:GetAnomalySubscriptions",
        "ce:GetApproximateUsageRecords",
        "ce:GetCommitmentPurchaseAnalysis",
        "ce:GetCostAndUsage",
        "ce:GetCostAndUsageComparisons",
        "ce:GetCostAndUsageWithResources",
        "ce:GetCostCategories",
        "ce:GetCostComparisonDrivers",
        "ce:GetCostForecast",
        "ce:GetDimensionValues",
        "ce:GetPreferences",
        "ce:GetReservationCoverage",
        "ce:GetReservationPurchaseRecommendation",
        "ce:GetReservationUtilization",
        "ce:GetRightsizingRecommendation",
        "ce:GetSavingsPlanPurchaseRecommendationDetails",
        "ce:GetSavingsPlansCoverage",
        "ce:GetSavingsPlansPurchaseRecommendation",
        "ce:GetSavingsPlansUtilization",
        "ce:GetSavingsPlansUtilizationDetails",
        "ce:GetTags",
        "ce:GetUsageForecast",
        "ce:ListCommitmentPurchaseAnalyses",
        "ce:ListCostAllocationTagBackfillHistory",
        "ce:ListCostAllocationTags",
        "ce:ListCostCategoryDefinitions",
        "ce:ListSavingsPlansPurchaseRecommendationGeneration",
        "ce:ListTagsForResource",
        "chatbot:Describe*",
```

```
        "chatbot:Get*",
        "chatbot:List*",
        "chime:Get*",
        "chime:List*",
        "chime:Retrieve*",
        "chime:Search*",
        "chime:Validate*",
        "cleanrooms-ml:GetAudienceGenerationJob",
        "cleanrooms-ml:GetAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModel",
        "cleanrooms-ml:GetConfiguredAudienceModelPolicy",
        "cleanrooms-ml:GetTrainingDataset",
        "cleanrooms-ml:ListAudienceExportJobs",
        "cleanrooms-ml:ListAudienceGenerationJobs",
        "cleanrooms-ml:ListAudienceModels",
        "cleanrooms-ml:ListConfiguredAudienceModels",
        "cleanrooms-ml:ListTagsForResource",
        "cleanrooms-ml:ListTrainingDatasets",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
```

```
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cleanrooms:GetCollaborationChangeRequest",
        "cleanrooms:GetProtectedJob",
        "cleanrooms:ListCollaborationChangeRequests",
        "cleanrooms:ListProtectedJobs",
        "cloud9:Describe*",
        "cloud9:List*",
        "clouddirectory:BatchRead",
        "clouddirectory:Get*",
        "clouddirectory:List*",
        "clouddirectory:LookupPolicy",
        "cloudformation:Describe*",
        "cloudformation:Detect*",
        "cloudformation:Estimate*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:ValidateTemplate",
        "cloudfront-keyvaluestore:Describe*",
        "cloudfront-keyvaluestore:Get*",
        "cloudfront-keyvaluestore:List*",
        "cloudfront:Describe*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudhsm:Describe*",
        "cloudhsm:GetResourcePolicy",
        "cloudhsm:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:Describe*",
        "cloudtrail:Get*",
```

```
        "cloudtrail:List*",
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GenerateQuery",
        "cloudwatch:GenerateQueryResultsSummary",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codeartifact:DescribeDomain",
        "codeartifact:DescribePackage",
        "codeartifact:DescribePackageVersion",
        "codeartifact:DescribeRepository",
        "codeartifact:GetAuthorizationToken",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetPackageVersionAsset",
        "codeartifact:GetPackageVersionReadme",
        "codeartifact:GetRepositoryEndpoint",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListDomains",
        "codeartifact:ListPackageVersionAssets",
        "codeartifact:ListPackageVersionDependencies",
        "codeartifact:ListPackageVersions",
        "codeartifact:ListPackages",
        "codeartifact:ListRepositories",
        "codeartifact:ListRepositoriesInDomain",
        "codeartifact:ListTagsForResource",
        "codeartifact:ReadFromRepository",
        "codebuild:BatchGet*",
        "codebuild:DescribeCodeCoverages",
        "codebuild:DescribeTestCases",
        "codebuild:List*",
        "codecatalyst:GetBillingAuthorization",
        "codecatalyst:GetConnection",
        "codecatalyst:GetPendingConnection",
        "codecatalyst:ListConnections",
        "codecatalyst:ListIamRolesForConnection",
        "codecatalyst:ListTagsForResource",
        "codecommit:BatchGet*",
        "codecommit:Describe*",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:List*",
        "codedeploy:BatchGet*",
        "codedeploy:Get*",
        "codedeploy:List*",
```

```
        "codeguru-profiler:Describe*",
        "codeguru-profiler:Get*",
        "codeguru-profiler:List*",
        "codeguru-reviewer:Describe*",
        "codeguru-reviewer:Get*",
        "codeguru-reviewer:List*",
        "codepipeline:Get*",
        "codepipeline:List*",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:GetRepositoryLink",
        "codestar-connections:GetRepositorySyncStatus",
        "codestar-connections:GetResourceSyncStatus",
        "codestar-connections:GetSyncConfiguration",
        "codestar-connections:ListConnections",
        "codestar-connections:ListHosts",
        "codestar-connections:ListRepositoryLinks",
        "codestar-connections:ListRepositorySyncDefinitions",
        "codestar-connections:ListSyncConfigurations",
        "codestar-connections:ListTagsForResource",
        "codestar-notifications:ListTargets",
        "codestar-notifications:describeNotificationRule",
        "codestar-notifications:listEventTypes",
        "codestar-notifications:listNotificationRules",
        "codestar-notifications:listTagsForResource",
        "codestar:Describe*",
        "codestar:Get*",
        "codestar:List*",
        "codestar:Verify*",
        "codewhisperer:ListProfiles",
        "cognito-identity:Describe*",
        "cognito-identity:GetCredentialsForIdentity",
        "cognito-identity:GetIdentityPoolAnalytics",
        "cognito-identity:GetIdentityPoolDailyAnalytics",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:GetIdentityProviderDailyAnalytics",
        "cognito-identity:GetOpenIdToken",
        "cognito-identity:GetOpenIdTokenForDeveloperIdentity",
        "cognito-identity:List*",
        "cognito-identity:Lookup*",
        "cognito-idp:AdminGet*",
        "cognito-idp:AdminList*",
        "cognito-idp:Describe*",
        "cognito-idp:Get*",
```

```
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:Get*",
        "cognito-sync:List*",
        "cognito-sync:QueryRecords",
        "comprehend:BatchDetect*",
        "comprehend:Classify*",
        "comprehend:Contains*",
        "comprehend:Describe*",
        "comprehend:Detect*",
        "comprehend:List*",
        "compute-optimizer:DescribeRecommendationExportJobs",
        "compute-optimizer:GetAutoScalingGroupRecommendations",
        "compute-optimizer:GetEBSVolumeRecommendations",
        "compute-optimizer:GetEC2InstanceRecommendations",
        "compute-optimizer:GetEC2RecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendationProjectedMetrics",
        "compute-optimizer:GetECSServiceRecommendations",
        "compute-optimizer:GetEffectiveRecommendationPreferences",
        "compute-optimizer:GetEnrollmentStatus",
        "compute-optimizer:GetEnrollmentStatusesForOrganization",
        "compute-optimizer:GetIdleRecommendations",
        "compute-optimizer:GetLambdaFunctionRecommendations",
        "compute-optimizer:GetLicenseRecommendations",
        "compute-optimizer:GetRDSDatabaseRecommendationProjectedMetrics",
        "compute-optimizer:GetRDSDatabaseRecommendations",
        "compute-optimizer:GetRecommendationPreferences",
        "compute-optimizer:GetRecommendationSummaries",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:Describe*",
        "connect:GetContactAttributes",
        "connect:GetCurrentMetricData",
        "connect:GetCurrentUserData",
        "connect:GetFederationToken",
        "connect:GetMetricData",
        "connect:GetMetricDataV2",
        "connect:GetTaskTemplate",
```

```
        "connect:GetTrafficDistribution",
        "connect:List*",
        "consoleapp:GetDeviceIdentity",
        "consoleapp:ListDeviceIdentities",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "controlcatalog:GetControl",
        "controlcatalog:ListCommonControls",
        "controlcatalog:ListControlMappings",
        "controlcatalog:ListControls",
        "controlcatalog:ListDomains",
        "controlcatalog:ListObjectives",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendationSummaries",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListEfficiencyMetrics",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "customer-verification:GetCustomerVerificationDetails",
        "customer-verification:GetCustomerVerificationEligibility",
        "databrew:DescribeDataset",
        "databrew:DescribeJob",
        "databrew:DescribeJobRun",
        "databrew:DescribeProject",
        "databrew:DescribeRecipe",
        "databrew:DescribeRuleset",
        "databrew:DescribeSchedule",
        "databrew:ListDatasets",
        "databrew:ListJobRuns",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "databrew:ListRecipeVersions",
        "databrew:ListRecipes",
        "databrew:ListRulesets",
        "databrew:ListSchedules",
        "databrew:ListTagsForResource",
        "dataexchange:Get*",
        "dataexchange:List*",
        "datapipeline:Describe*",
        "datapipeline:EvaluateExpression",
        "datapipeline:Get*",
```

```
        "datapipeline:List*",
        "datapipeline:QueryObjects",
        "datapipeline:Validate*",
        "datasync:Describe*",
        "datasync:List*",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainSharingPolicy",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
        "datazone:GetProject",
        "datazone:GetProjectProfile",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListDomains",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
```

```
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjectProfiles",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTagsForResource",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "dax:BatchGetItem",
        "dax:Describe*",
        "dax:GetItem",
        "dax:ListTags",
        "dax:Query",
        "dax:Scan",
        "deadline:BatchGetJobEntity",
        "deadline:GetApplicationVersion",
        "deadline:GetBudget",
        "deadline:GetFarm",
        "deadline:GetFleet",
        "deadline:GetJob",
        "deadline:GetLicenseEndpoint",
        "deadline:GetMonitor",
        "deadline:GetQueue",
        "deadline:GetQueueEnvironment",
        "deadline:GetQueueFleetAssociation",
        "deadline:GetSession",
        "deadline:GetSessionAction",
        "deadline:GetSessionsStatisticsAggregation",
        "deadline:GetStep",
```

```
        "deadline:GetStorageProfile",
        "deadline:GetStorageProfileForQueue",
        "deadline:GetTask",
        "deadline:GetWorker",
        "deadline:ListAvailableMeteredProducts",
        "deadline:ListBudgets",
        "deadline:ListFarmMembers",
        "deadline:ListFarms",
        "deadline:ListFleetMembers",
        "deadline:ListFleets",
        "deadline:ListJobMembers",
        "deadline:ListJobParameterDefinitions",
        "deadline:ListJobs",
        "deadline:ListLicenseEndpoints",
        "deadline:ListMeteredProducts",
        "deadline:ListMonitors",
        "deadline:ListQueueEnvironments",
        "deadline:ListQueueFleetAssociations",
        "deadline:ListQueueMembers",
        "deadline:ListQueues",
        "deadline:ListSessionActions",
        "deadline:ListSessions",
        "deadline:ListSessionsForWorker",
        "deadline:ListStepConsumers",
        "deadline:ListStepDependencies",
        "deadline:ListSteps",
        "deadline:ListStorageProfiles",
        "deadline:ListStorageProfilesForQueue",
        "deadline:ListTagsForResource",
        "deadline:ListTasks",
        "deadline:ListWorkers",
        "deadline:SearchJobs",
        "deadline:SearchSteps",
        "deadline:SearchTasks",
        "deadline:SearchWorkers",
        "deepcomposer:GetComposition",
        "deepcomposer:GetModel",
        "deepcomposer:GetSampleModel",
        "deepcomposer:ListCompositions",
        "deepcomposer:ListModels",
        "deepcomposer:ListSampleModels",
        "deepcomposer:ListTrainingTopics",
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
```

```
        "detective:Get*",
        "detective:List*",
        "detective:SearchGraph",
        "devicefarm:Get*",
        "devicefarm:List*",
        "devops-guru:DescribeAccountHealth",
        "devops-guru:DescribeAccountOverview",
        "devops-guru:DescribeAnomaly",
        "devops-guru:DescribeEventSourcesConfig",
        "devops-guru:DescribeFeedback",
        "devops-guru:DescribeInsight",
        "devops-guru:DescribeOrganizationHealth",
        "devops-guru:DescribeOrganizationOverview",
        "devops-guru:DescribeOrganizationResourceCollectionHealth",
        "devops-guru:DescribeResourceCollectionHealth",
        "devops-guru:DescribeServiceIntegration",
        "devops-guru:GetCostEstimation",
        "devops-guru:GetResourceCollection",
        "devops-guru:ListAnomaliesForInsight",
        "devops-guru:ListAnomalousLogGroups",
        "devops-guru:ListEvents",
        "devops-guru:ListInsights",
        "devops-guru:ListMonitoredResources",
        "devops-guru:ListNotificationChannels",
        "devops-guru:ListOrganizationInsights",
        "devops-guru:ListRecommendations",
        "devops-guru:SearchInsights",
        "devops-guru:StartCostEstimation",
        "directconnect:Describe*",
        "discovery:Describe*",
        "discovery:Get*",
        "discovery:List*",
        "dlm:Get*",
        "dms:Describe*",
        "dms:List*",
        "dms:Test*",
        "docdb-elastic:ListClusters",
        "docdb-elastic:ListClusterSnapshots",
        "docdb-elastic:ListPendingMaintenanceActions",
        "docdb-elastic:ListTagsForResource",
        "drs:DescribeJobLogItems",
        "drs:DescribeJobs",
        "drs:DescribeLaunchConfigurationTemplates",
        "drs:DescribeRecoveryInstances",
```

```
        "drs:DescribeRecoverySnapshots",
        "drs:DescribeReplicationConfigurationTemplates",
        "drs:DescribeSourceNetworks",
        "drs:DescribeSourceServers",
        "drs:GetFailbackReplicationConfiguration",
        "drs:GetLaunchConfiguration",
        "drs:GetReplicationConfiguration",
        "drs:ListExtensibleSourceServers",
        "drs:ListLaunchActions",
        "drs:ListStagingAccounts",
        "drs:ListTagsForResource",
        "ds:Check*",
        "ds:Describe*",
        "ds:Get*",
        "ds:List*",
        "ds:Verify*",
        "dsql:GetCluster",
        "dsql:GetVpcEndpointServiceName",
        "dsql:ListClusters",
        "dsql:ListTagsForResource",
        "dynamodb:BatchGet*",
        "dynamodb:Describe*",
        "dynamodb:Get*",
        "dynamodb:List*",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "dynamodb:Scan",
        "ec2:Describe*",
        "ec2:DescribeInstanceImageMetadata",
        "ec2:Get*",
        "ec2:ListImagesInRecycleBin",
        "ec2:ListSnapshotsInRecycleBin",
        "ec2:SearchLocalGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ec2messages:Get*",
        "ecr-public:BatchCheckLayerAvailability",
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeImages",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetAuthorizationToken",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
```

```
        "ecr-public:ListTagsForResource",
        "ecr:BatchCheck*",
        "ecr:BatchGet*",
        "ecr:Describe*",
        "ecr:Get*",
        "ecr:List*",
        "ecs:Describe*",
        "ecs:List*",
        "eks:Describe*",
        "eks:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:Request*",
        "elasticbeanstalk:Retrieve*",
        "elasticbeanstalk:Validate*",
        "elasticfilesystem:Describe*",
        "elasticfilesystem:ListTagsForResource",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:List*",
        "elasticmapreduce:View*",
        "elastictranscoder:List*",
        "elastictranscoder:Read*",
        "elemental-appliances-software:Get*",
        "elemental-appliances-software:List*",
        "emr-containers:DescribeJobRun",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:ListJobRuns",
        "emr-containers:ListManagedEndpoints",
        "emr-containers:ListTagsForResource",
        "emr-containers:ListVirtualClusters",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "emr-serverless:ListTagsForResource",
        "es:Describe*",
        "es:ESHttpGet",
```

```
        "es:ESHttpHead",
        "es:Get*",
        "es:List*",
        "events:Describe*",
        "events:List*",
        "events:Test*",
        "evidently:GetExperiment",
        "evidently:GetExperimentResults",
        "evidently:GetFeature",
        "evidently:GetLaunch",
        "evidently:GetProject",
        "evidently:GetSegment",
        "evidently:ListExperiments",
        "evidently:ListFeatures",
        "evidently:ListLaunches",
        "evidently:ListProjects",
        "evidently:ListSegmentReferences",
        "evidently:ListSegments",
        "evidently:ListTagsForResource",
        "evidently:TestSegmentPattern",
        "firehose:Describe*",
        "firehose:List*",
        "fis:GetAction",
        "fis:GetExperiment",
        "fis:GetExperimentTargetAccountConfiguration",
        "fis:GetExperimentTemplate",
        "fis:GetTargetAccountConfiguration",
        "fis:GetTargetResourceType",
        "fis:ListActions",
        "fis:ListExperimentResolvedTargets",
        "fis:ListExperimentTargetAccountConfigurations",
        "fis:ListExperimentTemplates",
        "fis:ListExperiments",
        "fis:ListTagsForResource",
        "fis:ListTargetAccountConfigurations",
        "fis:ListTargetResourceTypes",
        "fms:GetAdminAccount",
        "fms:GetAdminScope",
        "fms:GetAppsList",
        "fms:GetComplianceDetail",
        "fms:GetNotificationChannel",
        "fms:GetPolicy",
        "fms:GetProtectionStatus",
        "fms:GetProtocolsList",
```

```
        "fms:GetViolationDetails",
        "fms:ListAppsLists",
        "fms:ListComplianceStatus",
        "fms:ListMemberAccounts",
        "fms:ListPolicies",
        "fms:ListProtocolsLists",
        "fms:ListTagsForResource",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeExplainability",
        "forecast:DescribeExplainabilityExport",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:DescribeMonitor",
        "forecast:DescribePredictor",
        "forecast:DescribePredictorBacktestExportJob",
        "forecast:DescribeWhatIfAnalysis",
        "forecast:DescribeWhatIfForecast",
        "forecast:DescribeWhatIfForecastExport",
        "forecast:GetAccuracyMetrics",
        "forecast:ListDatasetGroups",
        "forecast:ListDatasetImportJobs",
        "forecast:ListDatasets",
        "forecast:ListExplainabilities",
        "forecast:ListExplainabilityExports",
        "forecast:ListForecastExportJobs",
        "forecast:ListForecasts",
        "forecast:ListMonitorEvaluations",
        "forecast:ListMonitors",
        "forecast:ListPredictorBacktestExportJobs",
        "forecast:ListPredictors",
        "forecast:ListWhatIfAnalyses",
        "forecast:ListWhatIfForecastExports",
        "forecast:ListWhatIfForecasts",
        "forecast:QueryForecast",
        "forecast:QueryWhatIfForecast",
        "frauddetector:BatchGetVariable",
        "frauddetector:DescribeDetector",
        "frauddetector:DescribeModelVersions",
        "frauddetector:GetBatchImportJobs",
        "frauddetector:GetBatchPredictionJobs",
        "frauddetector:GetDeleteEventsByEventTypeStatus",
```

```
        "frauddetector:GetDetectorVersion",
        "frauddetector:GetDetectors",
        "frauddetector:GetEntityTypes",
        "frauddetector:GetEvent",
        "frauddetector:GetEventPredictionMetadata",
        "frauddetector:GetEventTypes",
        "frauddetector:GetExternalModels",
        "frauddetector:GetKMSEncryptionKey",
        "frauddetector:GetLabels",
        "frauddetector:GetListElements",
        "frauddetector:GetListsMetadata",
        "frauddetector:GetModelVersion",
        "frauddetector:GetModels",
        "frauddetector:GetOutcomes",
        "frauddetector:GetRules",
        "frauddetector:GetVariables",
        "frauddetector:ListEventPredictions",
        "frauddetector:ListTagsForResource",
        "freertos:Describe*",
        "freertos:List*",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "freetier:GetAccountActivity",
        "freetier:GetAccountPlanState",
        "freetier:ListAccountActivities",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:Describe*",
        "gamelift:Get*",
        "gamelift:List*",
        "gamelift:ResolveAlias",
        "gamelift:Search*",
        "glacier:Describe*",
        "glacier:Get*",
        "glacier:List*",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:BatchGetCrawlers",
        "glue:BatchGetDevEndpoints",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchGetTriggers",
        "glue:BatchGetWorkflows",
```

```
        "glue:CheckSchemaVersionValidity",
        "glue:GetCatalogImportStatus",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetCrawler",
        "glue:GetCrawlerMetrics",
        "glue:GetCrawlers",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataflowGraph",
        "glue:GetDevEndpoint",
        "glue:GetDevEndpoints",
        "glue:GetJob",
        "glue:GetJobBookmark",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:GetJobs",
        "glue:GetMLTaskRun",
        "glue:GetMLTaskRuns",
        "glue:GetMLTransform",
        "glue:GetMLTransforms",
        "glue:GetMapping",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:GetPlan",
        "glue:GetRegistry",
        "glue:GetResourcePolicy",
        "glue:GetSchema",
        "glue:GetSchemaByDefinition",
        "glue:GetSchemaVersion",
        "glue:GetSchemaVersionsDiff",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:GetTags",
        "glue:GetTrigger",
        "glue:GetTriggers",
```

```
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions",
        "glue:GetWorkflow",
        "glue:GetWorkflowRun",
        "glue:GetWorkflowRunProperties",
        "glue:GetWorkflowRuns",
        "glue:ListCrawlers",
        "glue:ListCrawls",
        "glue:ListDevEndpoints",
        "glue:ListJobs",
        "glue:ListMLTransforms",
        "glue:ListRegistries",
        "glue:ListSchemaVersions",
        "glue:ListSchemas",
        "glue:ListSessions",
        "glue:ListStatements",
        "glue:ListTableOptimizerRuns",
        "glue:ListTriggers",
        "glue:ListWorkflows",
        "glue:QuerySchemaVersionMetadata",
        "glue:SearchTables",
        "grafana:DescribeWorkspace",
        "grafana:DescribeWorkspaceAuthentication",
        "grafana:DescribeWorkspaceConfiguration",
        "grafana:ListPermissions",
        "grafana:ListTagsForResource",
        "grafana:ListVersions",
        "grafana:ListWorkspaces",
        "greengrass:DescribeComponent",
        "greengrass:Get*",
        "greengrass:List*",
        "groundstation:DescribeContact",
        "groundstation:GetConfig",
        "groundstation:GetDataflowEndpointGroup",
        "groundstation:GetMinuteUsage",
        "groundstation:GetMissionProfile",
        "groundstation:GetSatellite",
        "groundstation:ListConfigs",
        "groundstation:ListContacts",
        "groundstation:ListDataflowEndpointGroups",
        "groundstation:ListGroundStations",
        "groundstation:ListMissionProfiles",
        "groundstation:ListSatellites",
        "groundstation:ListTagsForResource",
```

```
        "guardduty:Describe*",
        "guardduty:Get*",
        "guardduty:List*",
        "health:Describe*",
        "healthlake:DescribeFHIRDatastore",
        "healthlake:DescribeFHIRExportJob",
        "healthlake:DescribeFHIRImportJob",
        "healthlake:GetCapabilities",
        "healthlake:ListFHIRDatastores",
        "healthlake:ListFHIRExportJobs",
        "healthlake:ListFHIRImportJobs",
        "healthlake:ListTagsForResource",
        "healthlake:ReadResource",
        "healthlake:SearchWithGet",
        "healthlake:SearchWithPost",
        "iam:Generate*",
        "iam:Get*",
        "iam:List*",
        "iam:Simulate*",
        "identity-sync:GetSyncProfile",
        "identity-sync:GetSyncTarget",
        "identity-sync:ListSyncFilters",
        "identitystore-auth:BatchGetSession",
        "identitystore-auth:ListSessions",
        "identitystore:DescribeGroup",
        "identitystore:DescribeGroupMembership",
        "identitystore:DescribeUser",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "imagebuilder:Get*",
        "imagebuilder:List*",
        "importexport:Get*",
        "importexport:List*",
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetCodeSnippet",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:BatchGetMemberEc2DeepInspectionStatus",
        "inspector2:DescribeOrganizationConfiguration",
```

```
        "inspector2:GetCisScanReport",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetEc2DeepInspectionConfiguration",
        "inspector2:GetEncryptionKey",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:GetSbomExport",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCisScanConfigurations",
        "inspector2:ListCisScans",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListMembers",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "inspector2:SearchVulnerabilities",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
        "internetmonitor:GetHealthEvent",
        "internetmonitor:GetInternetEvent",
        "internetmonitor:GetMonitor",
        "internetmonitor:ListHealthEvents",
        "internetmonitor:ListInternetEvents",
        "internetmonitor:ListMonitors",
        "internetmonitor:ListTagsForResource",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "iot1click:DescribeDevice",
        "iot1click:DescribePlacement",
        "iot1click:DescribeProject",
        "iot1click:GetDeviceMethods",
        "iot1click:GetDevicesInPlacement",
        "iot1click:ListDeviceEvents",
        "iot1click:ListDevices",
        "iot1click:ListPlacements",
        "iot1click:ListProjects",
```

```
        "iot1click:ListTagsForResource",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "iotanalytics:Describe*",
        "iotanalytics:Get*",
        "iotanalytics:List*",
        "iotanalytics:SampleChannelData",
        "iotevents:DescribeAlarm",
        "iotevents:DescribeAlarmModel",
        "iotevents:DescribeDetector",
        "iotevents:DescribeDetectorModel",
        "iotevents:DescribeInput",
        "iotevents:DescribeLoggingOptions",
        "iotevents:ListAlarmModelVersions",
        "iotevents:ListAlarmModels",
        "iotevents:ListAlarms",
        "iotevents:ListDetectorModelVersions",
        "iotevents:ListDetectorModels",
        "iotevents:ListDetectors",
        "iotevents:ListInputs",
        "iotevents:ListTagsForResource",
        "iotfleethub:DescribeApplication",
        "iotfleethub:ListApplications",
        "iotfleetwise:GetCampaign",
        "iotfleetwise:GetDecoderManifest",
        "iotfleetwise:GetFleet",
        "iotfleetwise:GetLoggingOptions",
        "iotfleetwise:GetModelManifest",
        "iotfleetwise:GetRegisterAccountStatus",
        "iotfleetwise:GetSignalCatalog",
        "iotfleetwise:GetVehicle",
        "iotfleetwise:GetVehicleStatus",
        "iotfleetwise:ListCampaigns",
        "iotfleetwise:ListDecoderManifestNetworkInterfaces",
        "iotfleetwise:ListDecoderManifestSignals",
        "iotfleetwise:ListDecoderManifests",
        "iotfleetwise:ListFleets",
        "iotfleetwise:ListFleetsForVehicle",
        "iotfleetwise:ListModelManifestNodes",
        "iotfleetwise:ListModelManifests",
        "iotfleetwise:ListSignalCatalogNodes",
        "iotfleetwise:ListSignalCatalogs",
        "iotfleetwise:ListTagsForResource",
```

```
        "iotfleetwise:ListVehicles",
        "iotfleetwise:ListVehiclesInFleet",
        "iotsitewise:Describe*",
        "iotsitewise:Get*",
        "iotsitewise:List*",
        "iotwireless:GetDestination",
        "iotwireless:GetDeviceProfile",
        "iotwireless:GetEventConfigurationByResourceTypes",
        "iotwireless:GetFuotaTask",
        "iotwireless:GetLogLevelsByResourceTypes",
        "iotwireless:GetMetricConfiguration",
        "iotwireless:GetMetrics",
        "iotwireless:GetMulticastGroup",
        "iotwireless:GetMulticastGroupSession",
        "iotwireless:GetNetworkAnalyzerConfiguration",
        "iotwireless:GetPartnerAccount",
        "iotwireless:GetPosition",
        "iotwireless:GetPositionConfiguration",
        "iotwireless:GetPositionEstimate",
        "iotwireless:GetResourceEventConfiguration",
        "iotwireless:GetResourceLogLevel",
        "iotwireless:GetResourcePosition",
        "iotwireless:GetServiceEndpoint",
        "iotwireless:GetServiceProfile",
        "iotwireless:GetWirelessDevice",
        "iotwireless:GetWirelessDeviceImportTask",
        "iotwireless:GetWirelessDeviceStatistics",
        "iotwireless:GetWirelessGateway",
        "iotwireless:GetWirelessGatewayCertificate",
        "iotwireless:GetWirelessGatewayFirmwareInformation",
        "iotwireless:GetWirelessGatewayStatistics",
        "iotwireless:GetWirelessGatewayTask",
        "iotwireless:GetWirelessGatewayTaskDefinition",
        "iotwireless:ListDestinations",
        "iotwireless:ListDeviceProfiles",
        "iotwireless:ListDevicesForWirelessDeviceImportTask",
        "iotwireless:ListEventConfigurations",
        "iotwireless:ListFuotaTasks",
        "iotwireless:ListMulticastGroups",
        "iotwireless:ListMulticastGroupsByFuotaTask",
        "iotwireless:ListNetworkAnalyzerConfigurations",
        "iotwireless:ListPartnerAccounts",
        "iotwireless:ListPositionConfigurations",
        "iotwireless:ListQueuedMessages",
```

```
        "iotwireless:ListServiceProfiles",
        "iotwireless:ListTagsForResource",
        "iotwireless:ListWirelessDeviceImportTasks",
        "iotwireless:ListWirelessDevices",
        "iotwireless:ListWirelessGatewayTaskDefinitions",
        "iotwireless:ListWirelessGateways",
        "ivs:BatchGetChannel",
        "ivs:GetChannel",
        "ivs:GetComposition",
        "ivs:GetEncoderConfiguration",
        "ivs:GetIngestConfiguration",
        "ivs:GetParticipant",
        "ivs:GetPlaybackKeyPair",
        "ivs:GetPlaybackRestrictionPolicy",
        "ivs:GetPublicKey",
        "ivs:GetRecordingConfiguration",
        "ivs:GetStage",
        "ivs:GetStageSession",
        "ivs:GetStorageConfiguration",
        "ivs:GetStream",
        "ivs:GetStreamSession",
        "ivs:ListChannels",
        "ivs:ListCompositions",
        "ivs:ListEncoderConfigurations",
        "ivs:ListIngestConfigurations",
        "ivs:ListParticipantEvents",
        "ivs:ListParticipants",
        "ivs:ListPlaybackKeyPairs",
        "ivs:ListPlaybackRestrictionPolicies",
        "ivs:ListPublicKeys",
        "ivs:ListRecordingConfigurations",
        "ivs:ListStageSessions",
        "ivs:ListStages",
        "ivs:ListStorageConfigurations",
        "ivs:ListStreamKeys",
        "ivs:ListStreamSessions",
        "ivs:ListStreams",
        "ivs:ListTagsForResource",
        "ivschat:GetLoggingConfiguration",
        "ivschat:GetRoom",
        "ivschat:ListLoggingConfigurations",
        "ivschat:ListRooms",
        "ivschat:ListTagsForResource"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "ReadOnlyActionsGroup2",
      "Effect" : "Allow",
      "Action" : [
        "kafka:Describe*",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterOperation",
        "kafka:DescribeClusterV2",
        "kafka:DescribeConfiguration",
        "kafka:DescribeConfigurationRevision",
        "kafka:Get*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafka:ListClusterOperations",
        "kafka:ListClusters",
        "kafka:ListClustersV2",
        "kafka:ListConfigurationRevisions",
        "kafka:ListConfigurations",
        "kafka:ListKafkaVersions",
        "kafka:ListNodes",
        "kafka:ListTagsForResource",
        "kafkaconnect:DescribeConnector",
        "kafkaconnect:DescribeCustomPlugin",
        "kafkaconnect:DescribeWorkerConfiguration",
        "kafkaconnect:ListConnectors",
        "kafkaconnect:ListCustomPlugins",
        "kafkaconnect:ListWorkerConfigurations",
        "kendra:BatchGetDocumentStatus",
        "kendra:DescribeDataSource",
        "kendra:DescribeExperience",
        "kendra:DescribeFaq",
        "kendra:DescribeIndex",
        "kendra:DescribePrincipalMapping",
        "kendra:DescribeQuerySuggestionsBlockList",
        "kendra:DescribeQuerySuggestionsConfig",
        "kendra:DescribeThesaurus",
        "kendra:GetQuerySuggestions",
        "kendra:GetSnapshots",
        "kendra:ListDataSourceSyncJobs",
        "kendra:ListDataSources",
        "kendra:ListEntityPersonas",
```

```
        "kendra:ListExperienceEntities",
        "kendra:ListExperiences",
        "kendra:ListFaqs",
        "kendra:ListGroupsOlderThanOrderingId",
        "kendra:ListIndices",
        "kendra:ListQuerySuggestionsBlockLists",
        "kendra:ListTagsForResource",
        "kendra:ListThesauri",
        "kendra:Query",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kinesisanalytics:Describe*",
        "kinesisanalytics:Discover*",
        "kinesisanalytics:Get*",
        "kinesisanalytics:List*",
        "kinesisvideo:Describe*",
        "kinesisvideo:Get*",
        "kinesisvideo:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetEffectivePermissionsForPath",
        "lakeformation:GetLfTag",
        "lakeformation:GetResourceLfTags",
        "lakeformation:ListDataCellsFilter",
        "lakeformation:ListLfTags",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListTableStorageOptimizers",
        "lakeformation:SearchDatabasesByLfTags",
        "lakeformation:SearchTablesByLfTags",
        "lambda:Get*",
        "lambda:List*",
        "launchwizard:DescribeAdditionalNode",
        "launchwizard:DescribeProvisionedApp",
        "launchwizard:DescribeProvisioningEvents",
        "launchwizard:DescribeSettingsSet",
        "launchwizard:GetDeployment",
        "launchwizard:GetInfrastructureSuggestion",
        "launchwizard:GetIpAddress",
```

```
        "launchwizard:GetResourceCostEstimate",
        "launchwizard:GetResourceRecommendation",
        "launchwizard:GetSettingsSet",
        "launchwizard:GetWorkload",
        "launchwizard:GetWorkloadAsset",
        "launchwizard:GetWorkloadAssets",
        "launchwizard:GetWorkloadDeploymentPattern",
        "launchwizard:ListAdditionalNodes",
        "launchwizard:ListAllowedResources",
        "launchwizard:ListDeploymentEvents",
        "launchwizard:ListDeployments",
        "launchwizard:ListProvisionedApps",
        "launchwizard:ListResourceCostEstimates",
        "launchwizard:ListSettingsSets",
        "launchwizard:ListTagsForResource",
        "launchwizard:ListWorkloadDeploymentOptions",
        "launchwizard:ListWorkloadDeploymentPatterns",
        "launchwizard:ListWorkloads",
        "lex:DescribeBot",
        "lex:DescribeBotAlias",
        "lex:DescribeBotChannel",
        "lex:DescribeBotLocale",
        "lex:DescribeBotReplica",
        "lex:DescribeBotVersion",
        "lex:DescribeExport",
        "lex:DescribeImport",
        "lex:DescribeIntent",
        "lex:DescribeResourcePolicy",
        "lex:DescribeSlot",
        "lex:DescribeSlotType",
        "lex:Get*",
        "lex:ListBotAliasReplicas",
        "lex:ListBotAliases",
        "lex:ListBotChannels",
        "lex:ListBotLocales",
        "lex:ListBotReplicas",
        "lex:ListBotVersionReplicas",
        "lex:ListBotVersions",
        "lex:ListBots",
        "lex:ListBuiltInIntents",
        "lex:ListBuiltInSlotTypes",
        "lex:ListExports",
        "lex:ListImports",
        "lex:ListIntents",
```

```
        "lex:ListSlotTypes",
        "lex:ListSlots",
        "lex:ListTagsForResource",
        "license-manager:Get*",
        "license-manager:List*",
        "lightsail:GetActiveNames",
        "lightsail:GetAlarms",
        "lightsail:GetAutoSnapshots",
        "lightsail:GetBlueprints",
        "lightsail:GetBucketAccessKeys",
        "lightsail:GetBucketBundles",
        "lightsail:GetBucketMetricData",
        "lightsail:GetBuckets",
        "lightsail:GetBundles",
        "lightsail:GetCertificates",
        "lightsail:GetCloudFormationStackRecords",
        "lightsail:GetContainerAPIMetadata",
        "lightsail:GetContainerImages",
        "lightsail:GetContainerServiceDeployments",
        "lightsail:GetContainerServiceMetricData",
        "lightsail:GetContainerServicePowers",
        "lightsail:GetContainerServices",
        "lightsail:GetDisk",
        "lightsail:GetDiskSnapshot",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetDisks",
        "lightsail:GetDistributionBundles",
        "lightsail:GetDistributionLatestCacheReset",
        "lightsail:GetDistributionMetricData",
        "lightsail:GetDistributions",
        "lightsail:GetDomain",
        "lightsail:GetDomains",
        "lightsail:GetExportSnapshotRecords",
        "lightsail:GetInstance",
        "lightsail:GetInstanceMetricData",
        "lightsail:GetInstancePortStates",
        "lightsail:GetInstanceSnapshot",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetInstanceState",
        "lightsail:GetInstances",
        "lightsail:GetKeyPair",
        "lightsail:GetKeyPairs",
        "lightsail:GetLoadBalancer",
        "lightsail:GetLoadBalancerMetricData",
```

```
        "lightsail:GetLoadBalancerTlsCertificates",
        "lightsail:GetLoadBalancers",
        "lightsail:GetOperation",
        "lightsail:GetOperations",
        "lightsail:GetOperationsForResource",
        "lightsail:GetRegions",
        "lightsail:GetRelationalDatabase",
        "lightsail:GetRelationalDatabaseBlueprints",
        "lightsail:GetRelationalDatabaseBundles",
        "lightsail:GetRelationalDatabaseEvents",
        "lightsail:GetRelationalDatabaseLogEvents",
        "lightsail:GetRelationalDatabaseLogStreams",
        "lightsail:GetRelationalDatabaseMetricData",
        "lightsail:GetRelationalDatabaseParameters",
        "lightsail:GetRelationalDatabaseSnapshot",
        "lightsail:GetRelationalDatabaseSnapshots",
        "lightsail:GetRelationalDatabases",
        "lightsail:GetStaticIp",
        "lightsail:GetStaticIps",
        "lightsail:Is*",
        "logs:Describe*",
        "logs:FilterLogEvents",
        "logs:Get*",
        "logs:ListAnomalies",
        "logs:ListEntitiesForLogGroup",
        "logs:ListIntegrations",
        "logs:ListLogAnomalyDetectors",
        "logs:ListLogDeliveries",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "logs:StartLiveTail",
        "logs:StartQuery",
        "logs:StopLiveTail",
        "logs:StopQuery",
        "logs:TestMetricFilter",
        "logs:ListAggregateLogGroupSummaries",
        "logs:ListSourcesForS3TableIntegration",
        "logs:ListScheduledQueries",
        "lookoutequipment:DescribeDataIngestionJob",
        "lookoutequipment:DescribeDataset",
        "lookoutequipment:DescribeInferenceScheduler",
        "lookoutequipment:DescribeLabel",
```

```
        "lookoutequipment:DescribeLabelGroup",
        "lookoutequipment:DescribeModel",
        "lookoutequipment:DescribeModelVersion",
        "lookoutequipment:DescribeResourcePolicy",
        "lookoutequipment:DescribeRetrainingScheduler",
        "lookoutequipment:ListDataIngestionJobs",
        "lookoutequipment:ListDatasets",
        "lookoutequipment:ListInferenceEvents",
        "lookoutequipment:ListInferenceExecutions",
        "lookoutequipment:ListInferenceSchedulers",
        "lookoutequipment:ListLabelGroups",
        "lookoutequipment:ListLabels",
        "lookoutequipment:ListModelVersions",
        "lookoutequipment:ListModels",
        "lookoutequipment:ListRetrainingSchedulers",
        "lookoutequipment:ListSensorStatistics",
        "lookoutequipment:ListTagsForResource",
        "lookoutmetrics:Describe*",
        "lookoutmetrics:Get*",
        "lookoutmetrics:List*",
        "lookoutvision:DescribeDataset",
        "lookoutvision:DescribeModel",
        "lookoutvision:DescribeModelPackagingJob",
        "lookoutvision:DescribeProject",
        "lookoutvision:ListDatasetEntries",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "lookoutvision:ListTagsForResource",
        "m2:GetApplication",
        "m2:GetApplicationVersion",
        "m2:GetBatchJobExecution",
        "m2:GetDataSetDetails",
        "m2:GetDataSetImportTask",
        "m2:GetDeployment",
        "m2:GetEnvironment",
        "m2:ListApplicationVersions",
        "m2:ListApplications",
        "m2:ListBatchJobDefinitions",
        "m2:ListBatchJobExecutions",
        "m2:ListDataSetImportHistory",
        "m2:ListDataSets",
        "m2:ListDeployments",
        "m2:ListEngineVersions",
```

```
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "macie2:BatchGetCustomDataIdentifiers",
        "macie2:DescribeBuckets",
        "macie2:DescribeClassificationJob",
        "macie2:DescribeOrganizationConfiguration",
        "macie2:GetAdministratorAccount",
        "macie2:GetAllowList",
        "macie2:GetAutomatedDiscoveryConfiguration",
        "macie2:GetBucketStatistics",
        "macie2:GetClassificationExportConfiguration",
        "macie2:GetClassificationScope",
        "macie2:GetCustomDataIdentifier",
        "macie2:GetFindingStatistics",
        "macie2:GetFindings",
        "macie2:GetFindingsFilter",
        "macie2:GetFindingsPublicationConfiguration",
        "macie2:GetInvitationsCount",
        "macie2:GetMacieSession",
        "macie2:GetMember",
        "macie2:GetResourceProfile",
        "macie2:GetRevealConfiguration",
        "macie2:GetSensitiveDataOccurrencesAvailability",
        "macie2:GetSensitivityInspectionTemplate",
        "macie2:GetUsageStatistics",
        "macie2:GetUsageTotals",
        "macie2:ListAllowLists",
        "macie2:ListAutomatedDiscoveryAccounts",
        "macie2:ListClassificationJobs",
        "macie2:ListClassificationScopes",
        "macie2:ListCustomDataIdentifiers",
        "macie2:ListFindings",
        "macie2:ListFindingsFilters",
        "macie2:ListInvitations",
        "macie2:ListMembers",
        "macie2:ListOrganizationAdminAccounts",
        "macie2:ListResourceProfileArtifacts",
        "macie2:ListResourceProfileDetections",
        "macie2:ListSensitivityInspectionTemplates",
        "macie2:ListTagsForResource",
        "macie2:SearchResources",
        "managedblockchain:GetMember",
```

```
        "managedblockchain:GetNetwork",
        "managedblockchain:GetNode",
        "managedblockchain:GetProposal",
        "managedblockchain:ListInvitations",
        "managedblockchain:ListMembers",
        "managedblockchain:ListNetworks",
        "managedblockchain:ListNodes",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:ListProposals",
        "managedblockchain:ListTagsForResource",
        "mediaconnect:DescribeFlow",
        "mediaconnect:DescribeOffering",
        "mediaconnect:DescribeReservation",
        "mediaconnect:ListEntitlements",
        "mediaconnect:ListFlows",
        "mediaconnect:ListOfferings",
        "mediaconnect:ListReservations",
        "mediaconnect:ListTagsForResource",
        "mediaconvert:DescribeEndpoints",
        "mediaconvert:Get*",
        "mediaconvert:List*",
        "medialive:DescribeAccountConfiguration",
        "medialive:DescribeChannel",
        "medialive:DescribeChannelPlacementGroup",
        "medialive:DescribeCluster",
        "medialive:DescribeInput",
        "medialive:DescribeInputDevice",
        "medialive:DescribeInputDeviceThumbnail",
        "medialive:DescribeInputSecurityGroup",
        "medialive:DescribeMultiplex",
        "medialive:DescribeMultiplexProgram",
        "medialive:DescribeNetwork",
        "medialive:DescribeOffering",
        "medialive:DescribeReservation",
        "medialive:DescribeSchedule",
        "medialive:GetCloudWatchAlarmTemplate",
        "medialive:GetCloudWatchAlarmTemplateGroup",
        "medialive:GetEventBridgeRuleTemplate",
        "medialive:GetEventBridgeRuleTemplateGroup",
        "medialive:GetSignalMap",
        "medialive:ListChannels",
        "medialive:ListCloudWatchAlarmTemplateGroups",
        "medialive:ListCloudWatchAlarmTemplates",
        "medialive:ListEventBridgeRuleTemplateGroups",
```

```
        "medialive:ListEventBridgeRuleTemplates",
        "medialive:ListInputDevices",
        "medialive:ListInputDeviceTransfers",
        "medialive:ListInputs",
        "medialive:ListInputSecurityGroups",
        "medialive:ListMultiplexes",
        "medialive:ListMultiplexPrograms",
        "medialive:ListOfferings",
        "medialive:ListReservations",
        "medialive:ListSignalMaps",
        "medialive:ListTagsForResource",
        "mediapackage-vod:Describe*",
        "mediapackage-vod:List*",
        "mediapackage:Describe*",
        "mediapackage:List*",
        "mediapackagev2:GetChannel",
        "mediapackagev2:GetChannelGroup",
        "mediapackagev2:GetChannelPolicy",
        "mediapackagev2:GetHeadObject",
        "mediapackagev2:GetObject",
        "mediapackagev2:GetOriginEndpoint",
        "mediapackagev2:GetOriginEndpointPolicy",
        "mediapackagev2:ListChannelGroups",
        "mediapackagev2:ListChannels",
        "mediapackagev2:ListOriginEndpoints",
        "mediapackagev2:ListTagsForResource",
        "mediastore:DescribeContainer",
        "mediastore:DescribeObject",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:GetLifecyclePolicy",
        "mediastore:GetMetricPolicy",
        "mediastore:GetObject",
        "mediastore:ListContainers",
        "mediastore:ListItems",
        "mediastore:ListTagsForResource",
        "memorydb:DescribeAcls",
        "memorydb:DescribeClusters",
        "memorydb:DescribeEngineVersions",
        "memorydb:DescribeEvents",
        "memorydb:DescribeMultiRegionClusters",
        "memorydb:DescribeMultiRegionParameterGroups",
        "memorydb:DescribeMultiRegionParameters",
        "memorydb:DescribeParameterGroups",
```

```
        "memorydb:DescribeParameters",
        "memorydb:DescribeReservedNodes",
        "memorydb:DescribeReservedNodesOfferings",
        "memorydb:DescribeServiceUpdates",
        "memorydb:DescribeSnapshots",
        "memorydb:DescribeSubnetGroups",
        "memorydb:DescribeUsers",
        "memorydb:ListAllowedMultiRegionClusterUpdates",
        "memorydb:ListAllowedNodeTypeUpdates",
        "memorydb:ListTags",
        "mgh:Describe*",
        "mgh:GetHomeRegion",
        "mgh:List*",
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:DescribeSourceServers",
        "mgn:DescribeVcenterClients",
        "mgn:GetLaunchConfiguration",
        "mgn:GetReplicationConfiguration",
        "mgn:ListApplications",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListWaves",
        "mobileanalytics:Get*",
        "mobiletargeting:Get*",
        "mobiletargeting:List*",
        "monitron:GetProject",
        "monitron:GetProjectAdminUser",
        "monitron:ListProjects",
        "monitron:ListTagsForResource",
        "mpa:GetApprovalTeam",
        "mpa:GetIdentitySource",
        "mpa:GetPolicyVersion",
        "mpa:GetResourcePolicy",
        "mpa:GetSession",
        "mpa:ListApprovalTeams",
        "mpa:ListIdentitySources",
        "mpa:ListPolicies",
        "mpa:ListPolicyVersions",
        "mpa:ListResourcePolicies",
        "mpa:ListSessions",
        "mpa:ListTagsForResource",
```

```
        "mq:Describe*",
        "mq:List*",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:DescribeTLSInspectionConfiguration",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "network-firewall:ListTLSInspectionConfigurations",
        "network-firewall:ListTagsForResource",
        "networkflowmonitor:GetMonitor",
        "networkflowmonitor:GetScope",
        "networkflowmonitor:ListMonitors",
        "networkflowmonitor:ListScopes",
        "networkmanager:DescribeGlobalNetworks",
        "networkmanager:GetConnectAttachment",
        "networkmanager:GetConnectPeer",
        "networkmanager:GetConnectPeerAssociations",
        "networkmanager:GetConnections",
        "networkmanager:GetCoreNetwork",
        "networkmanager:GetCoreNetworkChangeEvents",
        "networkmanager:GetCoreNetworkChangeSet",
        "networkmanager:GetCoreNetworkPolicy",
        "networkmanager:GetCustomerGatewayAssociations",
        "networkmanager:GetDevices",
        "networkmanager:GetLinkAssociations",
        "networkmanager:GetLinks",
        "networkmanager:GetNetworkResourceCounts",
        "networkmanager:GetNetworkResourceRelationships",
        "networkmanager:GetNetworkResources",
        "networkmanager:GetNetworkRoutes",
        "networkmanager:GetNetworkTelemetry",
        "networkmanager:GetResourcePolicy",
        "networkmanager:GetRouteAnalysis",
        "networkmanager:GetSiteToSiteVpnAttachment",
        "networkmanager:GetSites",
        "networkmanager:GetTransitGatewayConnectPeerAssociations",
        "networkmanager:GetTransitGatewayPeering",
        "networkmanager:GetTransitGatewayRegistrations",
        "networkmanager:GetTransitGatewayRouteTableAttachment",
```

```
        "networkmanager:GetVpcAttachment",
        "networkmanager:ListAttachments",
        "networkmanager:ListConnectPeers",
        "networkmanager:ListCoreNetworkPolicyVersions",
        "networkmanager:ListCoreNetworks",
        "networkmanager:ListPeerings",
        "networkmanager:ListTagsForResource",
        "networkmonitor:GetMonitor",
        "networkmonitor:GetProbe",
        "networkmonitor:ListMonitors",
        "networkmonitor:ListTagsForResource",
        "nimble:GetEula",
        "nimble:GetFeatureMap",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileMember",
        "nimble:GetStreamingImage",
        "nimble:GetStreamingSession",
        "nimble:GetStudio",
        "nimble:GetStudioComponent",
        "nimble:GetStudioMember",
        "nimble:ListEulaAcceptances",
        "nimble:ListEulas",
        "nimble:ListLaunchProfileMembers",
        "nimble:ListLaunchProfiles",
        "nimble:ListStreamingImages",
        "nimble:ListStreamingSessions",
        "nimble:ListStudioComponents",
        "nimble:ListStudioMembers",
        "nimble:ListStudios",
        "nimble:ListTagsForResource",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:ListTagsForResource",
        "notifications:GetEventRule",
        "notifications:GetFeatureOptInStatus",
        "notifications:GetManagedNotificationChildEvent",
        "notifications:GetManagedNotificationConfiguration",
        "notifications:GetManagedNotificationEvent",
        "notifications:GetNotificationConfiguration",
        "notifications:GetNotificationEvent",
        "notifications:GetNotificationsAccessForOrganization",
        "notifications:List*",
```

```
        "oam:GetLink",
        "oam:GetSink",
        "oam:GetSinkPolicy",
        "oam:ListAttachedLinks",
        "oam:ListLinks",
        "oam:ListSinks",
        "observabilityadmin:GetCentralizationRuleForOrganization",
        "observabilityadmin:GetTelemetryEnrichmentStatus",
        "observabilityadmin:GetTelemetryEvaluationStatus",
        "observabilityadmin:GetTelemetryEvaluationStatusForOrganization",
        "observabilityadmin:GetTelemetryRule",
        "observabilityadmin:GetTelemetryRuleForOrganization",
        "observabilityadmin:ListCentralizationRulesForOrganization",
        "observabilityadmin:ListResourceTelemetry",
        "observabilityadmin:ListResourceTelemetryForOrganization",
        "observabilityadmin:ListTagsForResource",
        "observabilityadmin:ListTelemetryRules",
        "observabilityadmin:ListTelemetryRulesForOrganization",
        "observabilityadmin:GetTelemetryPipeline",
        "observabilityadmin:ListTelemetryPipelines",
        "observabilityadmin:TestTelemetryPipeline",
        "observabilityadmin:ValidateTelemetryPipelineConfiguration",
        "observabilityadmin:ListS3TableIntegrations",
        "observabilityadmin:GetS3TableIntegration",
        "omics:Get*",
        "omics:List*",
        "one:GetDeviceConfigurationTemplate",
        "one:GetDeviceInstance",
        "one:GetDeviceInstanceConfiguration",
        "one:GetSite",
        "one:GetSiteAddress",
        "one:ListDeviceConfigurationTemplates",
        "one:ListDeviceInstances",
        "one:ListSites",
        "one:ListUsers",
        "opsworks-cm:Describe*",
        "opsworks-cm:List*",
        "opsworks:Describe*",
        "opsworks:Get*",
        "organizations:Describe*",
        "organizations:List*",
        "osis:GetPipeline",
        "osis:GetPipelineBlueprint",
        "osis:GetPipelineChangeProgress",
```

```
        "osis:ListPipelineBlueprints",
        "osis:ListPipelines",
        "osis:ListTagsForResource",
        "outposts:Get*",
        "outposts:List*",
        "payment-cryptography:GetAlias",
        "payment-cryptography:GetKey",
        "payment-cryptography:GetPublicKeyCertificate",
        "payment-cryptography:ListAliases",
        "payment-cryptography:ListKeys",
        "payment-cryptography:ListTagsForResource",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentInstruments",
        "payments:ListPaymentPreferences",
        "payments:ListPaymentProgramOptions",
        "payments:ListPaymentProgramStatus",
        "payments:ListTagsForResource",
        "pca-connector-ad:GetConnector",
        "pca-connector-ad:GetDirectoryRegistration",
        "pca-connector-ad:GetServicePrincipalName",
        "pca-connector-ad:GetTemplate",
        "pca-connector-ad:GetTemplateGroupAccessControlEntry",
        "pca-connector-ad:ListConnectors",
        "pca-connector-ad:ListDirectoryRegistrations",
        "pca-connector-ad:ListServicePrincipalNames",
        "pca-connector-ad:ListTagsForResource",
        "pca-connector-ad:ListTemplateGroupAccessControlEntries",
        "pca-connector-ad:ListTemplates",
        "pca-connector-scep:GetChallengeMetadata",
        "pca-connector-scep:GetConnector",
        "pca-connector-scep:ListChallengeMetadata",
        "pca-connector-scep:ListConnectors",
        "pca-connector-scep:ListTagsForResource",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:Describe*",
        "personalize:Get*",
        "personalize:List*",
```

```
            "pi:DescribeDimensionKeys",
            "pi:GetDimensionKeyDetails",
            "pi:GetResourceMetadata",
            "pi:GetResourceMetrics",
            "pi:ListAvailableResourceDimensions",
            "pi:ListAvailableResourceMetrics",
            "pipes:DescribePipe",
            "pipes:ListPipes",
            "pipes:ListTagsForResource",
            "polly:Describe*",
            "polly:Get*",
            "polly:List*",
            "polly:SynthesizeSpeech",
            "pricing:DescribeServices",
            "pricing:GetAttributeValues",
            "pricing:GetPriceListFileUrl",
            "pricing:GetProducts",
            "pricing:ListPriceLists",
            "proton:GetDeployment",
            "proton:GetEnvironment",
            "proton:GetEnvironmentTemplate",
            "proton:GetEnvironmentTemplateVersion",
            "proton:GetService",
            "proton:GetServiceInstance",
            "proton:GetServiceTemplate",
            "proton:GetServiceTemplateVersion",
            "proton:ListDeployments",
            "proton:ListEnvironmentAccountConnections",
            "proton:ListEnvironmentTemplates",
            "proton:ListEnvironments",
            "proton:ListServiceInstances",
            "proton:ListServiceTemplates",
            "proton:ListServices",
            "proton:ListTagsForResource",
            "purchase-orders:GetPurchaseOrder",
            "purchase-orders:ListPurchaseOrderInvoices",
            "purchase-orders:ListPurchaseOrders",
            "purchase-orders:ViewPurchaseOrders",
            "qbusiness:GetApplication",
            "qbusiness:GetChatControlsConfiguration",
            "qbusiness:GetDataSource",
            "qbusiness:GetGroup",
            "qbusiness:GetIndex",
            "qbusiness:GetPlugin",
```

```
        "qbusiness:GetRetriever",
        "qbusiness:GetUser",
        "qbusiness:GetWebExperience",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDataSources",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalKinesisStream",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:GetBlock",
        "qldb:GetDigest",
        "qldb:GetRevision",
        "qldb:ListJournalKinesisStreamsForLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "qldb:ListTagsForResource",
        "ram:Get*",
        "ram:List*",
        "rbin:GetRule",
        "rbin:ListRules",
        "rbin:ListTagsForResource",
        "rds:Describe*",
        "rds:Download*",
        "rds:List*",
        "redshift-serverless:GetCustomDomainAssociation",
        "redshift-serverless:GetEndpointAccess",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetRecoveryPoint",
        "redshift-serverless:GetResourcePolicy",
        "redshift-serverless:GetScheduledAction",
        "redshift-serverless:GetSnapshot",
        "redshift-serverless:GetTableRestoreStatus",
        "redshift-serverless:GetUsageLimit",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListCustomDomainAssociations",
        "redshift-serverless:ListEndpointAccess",
```

```
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListRecoveryPoints",
        "redshift-serverless:ListScheduledActions",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:ListSnapshots",
        "redshift-serverless:ListTableRestoreStatus",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListUsageLimits",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "redshift:GetReservedNodeExchangeOfferings",
        "redshift:ListRecommendations",
        "redshift:View*",
        "refactor-spaces:GetApplication",
        "refactor-spaces:GetEnvironment",
        "refactor-spaces:GetResourcePolicy",
        "refactor-spaces:GetRoute",
        "refactor-spaces:GetService",
        "refactor-spaces:ListApplications",
        "refactor-spaces:ListEnvironmentVpcs",
        "refactor-spaces:ListEnvironments",
        "refactor-spaces:ListRoutes",
        "refactor-spaces:ListServices",
        "refactor-spaces:ListTagsForResource",
        "rekognition:CompareFaces",
        "rekognition:DescribeDataset",
        "rekognition:DescribeProjectVersions",
        "rekognition:DescribeProjects",
        "rekognition:DescribeStreamProcessor",
        "rekognition:Detect*",
        "rekognition:GetCelebrityInfo",
        "rekognition:GetCelebrityRecognition",
        "rekognition:GetContentModeration",
        "rekognition:GetFaceDetection",
        "rekognition:GetFaceSearch",
        "rekognition:GetLabelDetection",
        "rekognition:GetPersonTracking",
        "rekognition:GetSegmentDetection",
        "rekognition:GetTextDetection",
        "rekognition:List*",
        "rekognition:RecognizeCelebrities",
        "rekognition:Search*",
        "resiliencehub:DescribeApp",
        "resiliencehub:DescribeAppAssessment",
```

```
        "resiliencehub:DescribeAppVersion",
        "resiliencehub:DescribeAppVersionAppComponent",
        "resiliencehub:DescribeAppVersionResource",
        "resiliencehub:DescribeAppVersionResourcesResolutionStatus",
        "resiliencehub:DescribeAppVersionTemplate",
        "resiliencehub:DescribeDraftAppVersionResourcesImportStatus",
        "resiliencehub:DescribeMetricsExport",
        "resiliencehub:DescribeResiliencyPolicy",
        "resiliencehub:DescribeResourceGroupingRecommendationTask",
        "resiliencehub:ListAlarmRecommendations",
        "resiliencehub:ListAppAssessmentComplianceDrifts",
        "resiliencehub:ListAppAssessmentResourceDrifts",
        "resiliencehub:ListAppAssessments",
        "resiliencehub:ListAppComponentCompliances",
        "resiliencehub:ListAppComponentRecommendations",
        "resiliencehub:ListAppInputSources",
        "resiliencehub:ListAppVersionAppComponents",
        "resiliencehub:ListAppVersionResourceMappings",
        "resiliencehub:ListAppVersionResources",
        "resiliencehub:ListAppVersions",
        "resiliencehub:ListApps",
        "resiliencehub:ListMetrics",
        "resiliencehub:ListRecommendationTemplates",
        "resiliencehub:ListResiliencyPolicies",
        "resiliencehub:ListResourceGroupingRecommendations",
        "resiliencehub:ListSopRecommendations",
        "resiliencehub:ListSuggestedResiliencyPolicies",
        "resiliencehub:ListTagsForResource",
        "resiliencehub:ListTestRecommendations",
        "resiliencehub:ListUnsupportedAppVersionResources",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:GetAccountLevelServiceConfiguration",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:GetManagedView",
        "resource-explorer-2:GetResourceExplorerSetup",
        "resource-explorer-2:GetServiceIndex",
        "resource-explorer-2:GetServiceView",
        "resource-explorer-2:GetView",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListIndexesForMembers",
        "resource-explorer-2:ListManagedViews",
        "resource-explorer-2:ListServiceIndexes",
        "resource-explorer-2:ListServiceViews",
```

```
        "resource-explorer-2:ListStreamingAccessForServices",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:Search",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "robomaker:BatchDescribe*",
        "robomaker:Describe*",
        "robomaker:Get*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53-recovery-cluster:Get*",
        "route53-recovery-cluster:ListRoutingControls",
        "route53-recovery-control-config:Describe*",
        "route53-recovery-control-config:GetResourcePolicy",
        "route53-recovery-control-config:List*",
        "route53-recovery-readiness:Get*",
        "route53-recovery-readiness:List*",
        "route53:Get*",
        "route53:List*",
        "route53:Test*",
        "route53domains:Check*",
        "route53domains:Get*",
        "route53domains:List*",
        "route53domains:View*",
        "route53profiles:GetProfile",
        "route53profiles:GetProfileAssociation",
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
```

```
        "rum:GetAppMonitor",
        "rum:GetAppMonitorData",
        "rum:ListAppMonitors",
        "s3-object-lambda:GetObject",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectLegalHold",
        "s3-object-lambda:GetObjectRetention",
        "s3-object-lambda:GetObjectTagging",
        "s3-object-lambda:GetObjectVersion",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3-object-lambda:GetObjectVersionTagging",
        "s3-object-lambda:ListBucket",
        "s3-object-lambda:ListBucketMultipartUploads",
        "s3-object-lambda:ListBucketVersions",
        "s3-object-lambda:ListMultipartUploadParts",
        "s3-outposts:GetAccessPoint",
        "s3-outposts:GetAccessPointPolicy",
        "s3-outposts:GetBucket",
        "s3-outposts:GetBucketPolicy",
        "s3-outposts:GetBucketTagging",
        "s3-outposts:GetBucketVersioning",
        "s3-outposts:GetLifecycleConfiguration",
        "s3-outposts:GetObject",
        "s3-outposts:GetObjectTagging",
        "s3-outposts:GetObjectVersion",
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging",
        "s3-outposts:GetReplicationConfiguration",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListBucket",
        "s3-outposts:ListBucketMultipartUploads",
        "s3-outposts:ListBucketVersions",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListMultipartUploadParts",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListRegionalBuckets",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:Get*",
        "s3:List*",
        "s3vectors:GetIndex",
        "s3vectors:GetVectorBucket",
        "s3vectors:GetVectorBucketPolicy",
        "s3vectors:GetVectors",
```

```
        "s3vectors:ListIndexes",
        "s3vectors:ListVectorBuckets",
        "s3vectors:ListVectors",
        "s3vectors:QueryVectors",
        "s3tables:GetTable",
        "s3tables:GetTableBucket",
        "s3tables:GetTableBucketEncryption",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketReplication",
        "s3tables:GetTableBucketStorageClass",
        "s3tables:GetTableData",
        "s3tables:GetTableEncryption",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceJobStatus",
        "s3tables:GetTableMetadataLocation",
        "s3tables:GetTablePolicy",
        "s3tables:GetTableRecordExpirationConfiguration",
        "s3tables:GetTableRecordExpirationJobStatus",
        "s3tables:GetTableReplication",
        "s3tables:GetTableReplicationStatus",
        "s3tables:GetTableStorageClass",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:ListTables",
        "s3tables:ListTagsForResource",
        "s3tables:GetNamespace",
        "sagemaker:Describe*",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:List*",
        "sagemaker:Search",
        "savingsplans:DescribeSavingsPlanRates",
        "savingsplans:DescribeSavingsPlans",
        "savingsplans:DescribeSavingsPlansOfferingRates",
        "savingsplans:DescribeSavingsPlansOfferings",
        "savingsplans:ListTagsForResource",
        "scheduler:GetSchedule",
        "scheduler:GetScheduleGroup",
        "scheduler:ListScheduleGroups",
        "scheduler:ListSchedules",
        "scheduler:ListTagsForResource",
        "schemas:Describe*",
        "schemas:Get*",
        "schemas:List*",
```

```
        "schemas:Search*",
        "sdb:Get*",
        "sdb:List*",
        "sdb:Select*",
        "secretsmanager:Describe*",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:List*",
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "securitylake:GetDataLakeExceptionSubscription",
        "securitylake:GetDataLakeOrganizationConfiguration",
        "securitylake:GetDataLakeSources",
        "securitylake:GetSubscriber",
        "securitylake:ListDataLakeExceptions",
        "securitylake:ListDataLakes",
        "securitylake:ListLogSources",
        "securitylake:ListSubscribers",
        "securitylake:ListTagsForResource",
        "serverlessrepo:Get*",
        "serverlessrepo:List*",
        "serverlessrepo:SearchApplications",
        "servicecatalog:Describe*",
        "servicecatalog:GetApplication",
        "servicecatalog:GetAttributeGroup",
        "servicecatalog:List*",
        "servicecatalog:Scan*",
        "servicecatalog:Search*",
        "servicediscovery:DiscoverInstances",
        "servicediscovery:DiscoverInstancesRevision",
        "servicediscovery:Get*",
        "servicediscovery:List*",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
```

```
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "ses:BatchGetMetricData",
        "ses:Describe*",
        "ses:Get*",
        "ses:List*",
        "shield:Describe*",
        "shield:Get*",
        "shield:List*",
        "signer:DescribeSigningJob",
        "signer:GetSigningPlatform",
        "signer:GetSigningProfile",
        "signer:ListProfilePermissions",
        "signer:ListSigningJobs",
        "signer:ListSigningPlatforms",
        "signer:ListSigningProfiles",
        "signer:ListTagsForResource",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole",
        "sms-voice:DescribeAccountAttributes",
        "sms-voice:DescribeAccountLimits",
        "sms-voice:DescribeConfigurationSets",
        "sms-voice:DescribeKeywords",
        "sms-voice:DescribeOptOutLists",
        "sms-voice:DescribeOptedOutNumbers",
        "sms-voice:DescribePhoneNumbers",
        "sms-voice:DescribePools",
        "sms-voice:DescribeProtectConfigurations",
        "sms-voice:DescribeRegistrationAttachments",
        "sms-voice:DescribeRegistrationFieldDefinitions",
        "sms-voice:DescribeRegistrationFieldValues",
        "sms-voice:DescribeRegistrations",
        "sms-voice:DescribeRegistrationSectionDefinitions",
        "sms-voice:DescribeRegistrationTypeDefinitions",
        "sms-voice:DescribeRegistrationVersions",
        "sms-voice:DescribeSenderIds",
        "sms-voice:DescribeSpendLimits",
        "sms-voice:DescribeVerifiedDestinationNumbers",
        "sms-voice:ListPoolOriginationIdentities",
        "sms-voice:ListTagsForResource",
        "snowball:Describe*",
        "snowball:Get*",
        "snowball:List*",
```

```
            "sns:Check*",
            "sns:Get*",
            "sns:List*",
            "sqs:Get*",
            "sqs:List*",
            "sqs:Receive*",
            "ssm-contacts:DescribeEngagement",
            "ssm-contacts:DescribePage",
            "ssm-contacts:GetContact",
            "ssm-contacts:GetContactChannel",
            "ssm-contacts:ListContactChannels",
            "ssm-contacts:ListContacts",
            "ssm-contacts:ListEngagements",
            "ssm-contacts:ListPageReceipts",
            "ssm-contacts:ListPagesByContact",
            "ssm-contacts:ListPagesByEngagement",
            "ssm-incidents:GetIncidentRecord",
            "ssm-incidents:GetReplicationSet",
            "ssm-incidents:GetResourcePolicies",
            "ssm-incidents:GetResponsePlan",
            "ssm-incidents:GetTimelineEvent",
            "ssm-incidents:ListIncidentRecords",
            "ssm-incidents:ListRelatedItems",
            "ssm-incidents:ListReplicationSets",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:ListTagsForResource",
            "ssm-incidents:ListTimelineEvents",
            "ssm-quicksetup:GetConfiguration",
            "ssm-quicksetup:GetConfigurationManager",
            "ssm-quicksetup:GetServiceSettings",
            "ssm-quicksetup:ListConfigurationManagers",
            "ssm-quicksetup:ListConfigurations",
            "ssm-quicksetup:ListQuickSetupTypes",
            "ssm-quicksetup:ListTagsForResource",
            "ssm-sap:GetApplication",
            "ssm-sap:GetComponent",
            "ssm-sap:GetConfigurationCheckOperation",
            "ssm-sap:GetDatabase",
            "ssm-sap:GetOperation",
            "ssm-sap:GetResourcePermission",
            "ssm-sap:ListApplications",
            "ssm-sap:ListComponents",
            "ssm-sap:ListConfigurationCheckDefinitions",
            "ssm-sap:ListConfigurationCheckOperations",
```

```
        "ssm-sap:ListDatabases",
        "ssm-sap:ListOperationEvents",
        "ssm-sap:ListOperations",
        "ssm-sap:ListSubCheckResults",
        "ssm-sap:ListSubCheckRuleResults",
        "ssm-sap:ListTagsForResource",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "sso-directory:Describe*",
        "sso-directory:List*",
        "sso-directory:Search*",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "states:Describe*",
        "states:GetExecutionHistory",
        "states:List*",
        "states:ValidateStateMachineDefinition",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "sts:GetCallerIdentity",
        "sts:GetSessionToken",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportLevel",
        "support:DescribeSupportedLanguages",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "support:DescribeTrustedAdvisorChecks",
        "support:SearchForCases",
        "supportplans:GetSupportPlan",
        "supportplans:GetSupportPlanUpdateStatus",
        "supportplans:ListSupportPlanModifiers",
        "sustainability:GetCarbonFootprintSummary",
```

```
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
        "synthetics:Describe*",
        "synthetics:Get*",
        "synthetics:List*",
        "tag:DescribeReportCreation",
        "tag:Get*",
        "tax:GetExemptions",
        "tax:GetTaxInheritance",
        "tax:GetTaxInterview",
        "tax:GetTaxRegistration",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations",
        "timestream:DescribeBatchLoadTask",
        "timestream:DescribeDatabase",
        "timestream:DescribeEndpoints",
        "timestream:DescribeTable",
        "timestream:ListBatchLoadTasks",
        "timestream:ListDatabases",
        "timestream:ListMeasures",
        "timestream:ListTables",
        "timestream:ListTagsForResource",
        "tnb:GetSolFunctionInstance",
        "tnb:GetSolFunctionPackage",
        "tnb:GetSolFunctionPackageContent",
        "tnb:GetSolFunctionPackageDescriptor",
        "tnb:GetSolNetworkInstance",
        "tnb:GetSolNetworkOperation",
        "tnb:GetSolNetworkPackage",
        "tnb:GetSolNetworkPackageContent",
        "tnb:GetSolNetworkPackageDescriptor",
        "tnb:ListSolFunctionInstances",
        "tnb:ListSolFunctionPackages",
        "tnb:ListSolNetworkInstances",
        "tnb:ListSolNetworkOperations",
        "tnb:ListSolNetworkPackages",
        "tnb:ListTagsForResource",
        "transcribe:Get*",
        "transcribe:List*",
        "transfer:Describe*",
        "transfer:List*",
        "transfer:TestIdentityProvider",
```

```
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:GetTerminology",
        "translate:ListParallelData",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "trustedadvisor:Describe*",
        "trustedadvisor:GetOrganizationRecommendation",
        "trustedadvisor:GetRecommendation",
        "trustedadvisor:ListChecks",
        "trustedadvisor:ListOrganizationRecommendationAccounts",
        "trustedadvisor:ListOrganizationRecommendationResources",
        "trustedadvisor:ListOrganizationRecommendations",
        "trustedadvisor:ListRecommendationResources",
        "trustedadvisor:ListRecommendations",
        "user-subscriptions:ListApplicationClaims",
        "user-subscriptions:ListClaims",
        "user-subscriptions:ListUserSubscriptions",
        "uxc:GetAccountColor",
        "verifiedpermissions:GetIdentitySource",
        "verifiedpermissions:GetPolicy",
        "verifiedpermissions:GetPolicyStore",
        "verifiedpermissions:GetPolicyTemplate",
        "verifiedpermissions:GetSchema",
        "verifiedpermissions:IsAuthorized",
        "verifiedpermissions:IsAuthorizedWithToken",
        "verifiedpermissions:ListIdentitySources",
        "verifiedpermissions:ListPolicies",
        "verifiedpermissions:ListPolicyStores",
        "verifiedpermissions:ListPolicyTemplates",
        "vpc-lattice:GetAccessLogSubscription",
        "vpc-lattice:GetAuthPolicy",
        "vpc-lattice:GetListener",
        "vpc-lattice:GetResourceConfiguration",
        "vpc-lattice:GetResourceGateway",
        "vpc-lattice:GetResourcePolicy",
        "vpc-lattice:GetRule",
        "vpc-lattice:GetService",
        "vpc-lattice:GetServiceNetwork",
        "vpc-lattice:GetServiceNetworkResourceAssociation",
        "vpc-lattice:GetServiceNetworkServiceAssociation",
        "vpc-lattice:GetServiceNetworkVpcAssociation",
        "vpc-lattice:GetTargetGroup",
        "vpc-lattice:ListAccessLogSubscriptions",
```

```
        "vpc-lattice:ListListeners",
        "vpc-lattice:ListResourceConfigurations",
        "vpc-lattice:ListResourceEndpointAssociations",
        "vpc-lattice:ListResourceGateways",
        "vpc-lattice:ListRules",
        "vpc-lattice:ListServiceNetworkResourceAssociations",
        "vpc-lattice:ListServiceNetworkServiceAssociations",
        "vpc-lattice:ListServiceNetworkVpcAssociations",
        "vpc-lattice:ListServiceNetworks",
        "vpc-lattice:ListServiceNetworkVpcEndpointAssociations",
        "vpc-lattice:ListServices",
        "vpc-lattice:ListTagsForResource",
        "vpc-lattice:ListTargetGroups",
        "vpc-lattice:ListTargets",
        "waf-regional:Get*",
        "waf-regional:List*",
        "waf:Get*",
        "waf:List*",
        "wafv2:CheckCapacity",
        "wafv2:Describe*",
        "wafv2:Get*",
        "wafv2:List*",
        "wellarchitected:ExportLens",
        "wellarchitected:GetAnswer",
        "wellarchitected:GetConsolidatedReport",
        "wellarchitected:GetLens",
        "wellarchitected:GetLensReview",
        "wellarchitected:GetLensReviewReport",
        "wellarchitected:GetLensVersionDifference",
        "wellarchitected:GetMilestone",
        "wellarchitected:GetProfile",
        "wellarchitected:GetProfileTemplate",
        "wellarchitected:GetReviewTemplate",
        "wellarchitected:GetReviewTemplateAnswer",
        "wellarchitected:GetReviewTemplateLensReview",
        "wellarchitected:GetWorkload",
        "wellarchitected:List*",
        "workdocs:CheckAlias",
        "workdocs:Describe*",
        "workdocs:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
```

```
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserAccessLoggingSettings",
        "workspaces-web:ListUserSettings",
        "workspaces:Describe*",
        "xray:BatchGet*",
        "xray:Get*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorFullAccess

Beschreibung: Bietet vollen Zugriff auf Resource Groups und den Tag-Editor.

`ResourceGroupsandTagEditorFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ResourceGroupsandTagEditorFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 10. August 2023, 13:29 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources",
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsandTagEditorReadOnlyAccess

Beschreibung: Ermöglicht den Zugriff auf die Verwendung von Resource Groups und den Tag-Editor, ermöglicht jedoch keine Bearbeitung von Tags über den Tag-Editor.

`ResourceGroupsandTagEditorReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ResourceGroupsandTagEditorReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:39 UTC
- Bearbeitete Zeit: 10. August 2023, 13:42 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-groups:Get*",
        "resource-groups:List*",
        "resource-groups:Search*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "cloudformation:ListStacks"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsServiceRolePolicy

Beschreibung: Ermöglicht AWS Resource Groups, die AWS Dienste abzufragen, die Ihre Ressourcen besitzen, um die Gruppe zu behalten up-to-date

`ResourceGroupsServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 5. Januar 2023, 16:57 UTC
- Bearbeitete Zeit: 5. Januar 2023, 16:57 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ResourceGroupsServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources"
      ],
      "Resource" : "*"
    }
  ]
```

```
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ResourceGroupsTaggingAPITagUntagSupportedResources

Beschreibung: Bietet Berechtigungen zum Markieren und Aufheben von Tags für alle Ressourcen, die von der Resource Groups Tagging API unterstützt werden. Diese Richtlinie gewährt auch die erforderlichen Berechtigungen, um alle markierten oder zuvor markierten Ressourcen über die Resource Groups Tagging API abzurufen.

`ResourceGroupsTaggingAPITagUntagSupportedResources`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ResourceGroupsTaggingAPITagUntagSupportedResources` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. Oktober 2024, 11:11 UTC
- Bearbeitete Zeit: 11. Dezember 2024, 17:51 UTC
- ARN: `arn:aws:iam::aws:policy/ResourceGroupsTaggingAPITagUntagSupportedResources`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "a4b:TagResource",
        "a4b:UntagResource",
        "access-analyzer:TagResource",
        "access-analyzer:UntagResource",
        "acm-pca:TagCertificateAuthority",
        "acm-pca:UntagCertificateAuthority",
        "acm:AddTagsToCertificate",
        "acm:RemoveTagsFromCertificate",
        "amplify:TagResource",
        "amplify:UntagResource",
        "appconfig:TagResource",
        "appconfig:UntagResource",
        "appflow:TagResource",
        "appflow:UntagResource",
        "appmesh:TagResource",
        "appmesh:UntagResource",
        "appstream:TagResource",
        "appstream:UntagResource",
        "appsync:TagResource",
        "appsync:UntagResource",
        "athena:TagResource",
        "athena:UntagResource",
        "auditmanager:TagResource",
        "auditmanager:UntagResource",
        "autoscaling:CreateOrUpdateTags",
        "autoscaling:DeleteTags",
        "backup:TagResource",
        "backup:UntagResource",
        "batch:TagResource",
        "batch:UntagResource",
        "braket:TagResource",
        "braket:UntagResource",
```

```
        "cassandra:TagResource",
        "cassandra:UntagResource",
        "chime:TagResource",
        "chime:UntagResource",
        "cloud9:TagResource",
        "cloud9:UntagResource",
        "clouddirectory:TagResource",
        "clouddirectory:UntagResource",
        "cloudfront:TagResource",
        "cloudfront:UntagResource",
        "cloudhsm:TagResource",
        "cloudhsm:UntagResource",
        "cloudtrail:AddTags",
        "cloudtrail:RemoveTags",
        "cloudwatch:TagResource",
        "cloudwatch:UntagResource",
        "codeartifact:TagResource",
        "codeartifact:UntagResource",
        "codecommit:TagResource",
        "codecommit:UntagResource",
        "codedeploy:AddTagsToOnPremisesInstances",
        "codedeploy:RemoveTagsFromOnPremisesInstances",
        "codedeploy:TagResource",
        "codedeploy:UntagResource",
        "codeguru-profiler:TagResource",
        "codeguru-profiler:UntagResource",
        "codepipeline:TagResource",
        "codepipeline:UntagResource",
        "codestar-connections:TagResource",
        "codestar-connections:UntagResource",
        "codestar:TagProject",
        "codestar:UntagProject",
        "cognito-identity:TagResource",
        "cognito-identity:UntagResource",
        "cognito-idp:TagResource",
        "cognito-idp:UntagResource",
        "comprehend:TagResource",
        "comprehend:UntagResource",
        "config:TagResource",
        "config:UntagResource",
        "connect:TagResource",
        "connect:UntagResource",
        "dataexchange:TagResource",
        "dataexchange:UntagResource",
```

```
        "datapipeline:AddTags",
        "datapipeline:RemoveTags",
        "datasync:TagResource",
        "datasync:UntagResource",
        "deepcomposer:TagResource",
        "deepcomposer:UntagResource",
        "detective:TagResource",
        "detective:UntagResource",
        "devicefarm:TagResource",
        "devicefarm:UntagResource",
        "directconnect:TagResource",
        "directconnect:UntagResource",
        "dlm:TagResource",
        "dlm:UntagResource",
        "dms:AddTagsToResource",
        "dms:RemoveTagsFromResource",
        "dynamodb:TagResource",
        "dynamodb:UntagResource",
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ecr:TagResource",
        "ecr:UntagResource",
        "ecs:TagResource",
        "ecs:UntagResource",
        "eks:TagResource",
        "eks:UntagResource",
        "elastic-inference:TagResource",
        "elastic-inference:UntagResource",
        "elasticache:AddTagsToResource",
        "elasticache:RemoveTagsFromResource",
        "elasticbeanstalk:UpdateTagsForResource",
        "elasticfilesystem:CreateTags",
        "elasticfilesystem:DeleteTags",
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:RemoveTags",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:RemoveTags",
        "emr-containers:TagResource",
        "emr-containers:UntagResource",
        "es:AddTags",
        "es:RemoveTags",
        "events:TagResource",
        "events:UntagResource",
        "firehose:TagDeliveryStream",
```

```
        "firehose:UntagDeliveryStream",
        "fms:TagResource",
        "fms:UntagResource",
        "forecast:TagResource",
        "forecast:UntagResource",
        "frauddetector:TagResource",
        "frauddetector:UntagResource",
        "fsx:TagResource",
        "fsx:UntagResource",
        "gamelift:TagResource",
        "gamelift:UntagResource",
        "glacier:AddTagsToVault",
        "glacier:RemoveTagsFromVault",
        "globalaccelerator:TagResource",
        "globalaccelerator:UntagResource",
        "glue:TagResource",
        "glue:UntagResource",
        "greengrass:TagResource",
        "greengrass:UntagResource",
        "groundstation:TagResource",
        "groundstation:UntagResource",
        "guardduty:TagResource",
        "guardduty:UntagResource",
        "iam:TagInstanceProfile",
        "iam:TagMFADevice",
        "iam:TagOpenIDConnectProvider",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagSAMLProvider",
        "iam:TagServerCertificate",
        "iam:TagUser",
        "iam:UntagInstanceProfile",
        "iam:UntagMFADevice",
        "iam:UntagOpenIDConnectProvider",
        "iam:UntagPolicy",
        "iam:UntagRole",
        "iam:UntagSAMLProvider",
        "iam:UntagServerCertificate",
        "iam:UntagUser",
        "imagebuilder:TagResource",
        "imagebuilder:UntagResource",
        "inspector:ListTagsForResource",
        "inspector:SetTagsForResource",
        "iot1click:TagResource",
```

```
        "iot1click:UntagResource",
        "iot:TagResource",
        "iot:UntagResource",
        "iotanalytics:TagResource",
        "iotanalytics:UntagResource",
        "iotdeviceadvisor:TagResource",
        "iotdeviceadvisor:UntagResource",
        "iotevents:TagResource",
        "iotevents:UntagResource",
        "iotfleethub:TagResource",
        "iotfleethub:UntagResource",
        "iotsitewise:TagResource",
        "iotsitewise:UntagResource",
        "iottwinmaker:TagResource",
        "iottwinmaker:UntagResource",
        "iotwireless:TagResource",
        "iotwireless:UntagResource",
        "ivs:TagResource",
        "ivs:UntagResource",
        "kafka:TagResource",
        "kafka:UntagResource",
        "kendra:TagResource",
        "kendra:UntagResource",
        "kinesis:AddTagsToStream",
        "kinesis:RemoveTagsFromStream",
        "kinesisanalytics:TagResource",
        "kinesisanalytics:UntagResource",
        "kms:TagResource",
        "kms:UntagResource",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lex:TagResource",
        "lex:UntagResource",
        "license-manager:TagResource",
        "license-manager:UntagResource",
        "lightsail:TagResource",
        "lightsail:UntagResource",
        "logs:TagLogGroup",
        "logs:TagResource",
        "logs:UntagLogGroup",
        "logs:UntagResource",
        "lookoutequipment:TagResource",
        "lookoutequipment:UntagResource",
        "machinelearning:AddTags",
```

```
        "machinelearning:DeleteTags",
        "macie2:TagResource",
        "macie2:UntagResource",
        "managedblockchain:TagResource",
        "managedblockchain:UntagResource",
        "mediaconnect:TagResource",
        "mediaconnect:UntagResource",
        "mediaconvert:TagResource",
        "mediaconvert:UntagResource",
        "medialive:CreateTags",
        "medialive:DeleteTags",
        "mediapackage-vod:TagResource",
        "mediapackage-vod:UntagResource",
        "mediapackage:TagResource",
        "mediapackage:UntagResource",
        "mediatailor:TagResource",
        "mediatailor:UntagResource",
        "mobiletargeting:TagResource",
        "mobiletargeting:UntagResource",
        "mq:CreateTags",
        "mq:DeleteTags",
        "neptune-graph:TagResource",
        "neptune-graph:UntagResource",
        "network-firewall:TagResource",
        "network-firewall:UntagResource",
        "networkmanager:TagResource",
        "networkmanager:UntagResource",
        "opsworks-cm:TagResource",
        "opsworks-cm:UntagResource",
        "opsworks:TagResource",
        "opsworks:UntagResource",
        "organizations:TagResource",
        "organizations:UntagResource",
        "outposts:TagResource",
        "outposts:UntagResource",
        "qldb:TagResource",
        "qldb:UntagResource",
        "quicksight:TagResource",
        "quicksight:UntagResource",
        "ram:TagResource",
        "ram:UntagResource",
        "rds:AddTagsToResource",
        "rds:RemoveTagsFromResource",
        "redshift:CreateTags",
```

```
        "redshift:DeleteTags",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-groups:Tag",
        "resource-groups:Untag",
        "robomaker:TagResource",
        "robomaker:UntagResource",
        "route53:ChangeTagsForResource",
        "route53domains:DeleteTagsForDomain",
        "route53domains:UpdateTagsForDomain",
        "route53resolver:TagResource",
        "route53resolver:UntagResource",
        "s3:GetBucketTagging",
        "s3:GetJobTagging",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging",
        "s3:GetStorageLensConfigurationTagging",
        "s3:DeleteJobTagging",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:PutBucketTagging",
        "s3:PutJobTagging",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:PutStorageLensConfigurationTagging",
        "s3:DeleteStorageLensConfigurationTagging",
        "s3:TagResource",
        "s3:UntagResource",
        "sagemaker:AddTags",
        "sagemaker:DeleteTags",
        "savingsplans:TagResource",
        "savingsplans:UntagResource",
        "schemas:TagResource",
        "schemas:UntagResource",
        "secretsmanager:TagResource",
        "secretsmanager:UntagResource",
        "securityhub:TagResource",
        "securityhub:UntagResource",
        "servicediscovery:TagResource",
        "servicediscovery:UntagResource",
        "servicequotas:TagResource",
        "servicequotas:UntagResource",
        "ses:TagResource",
        "ses:UntagResource",
```

```
            "sns:TagResource",
            "sns:UntagResource",
            "sqs:TagQueue",
            "sqs:UntagQueue",
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource",
            "states:TagResource",
            "states:UntagResource",
            "storagegateway:AddTagsToResource",
            "storagegateway:RemoveTagsFromResource",
            "swf:TagResource",
            "swf:UntagResource",
            "synthetics:TagResource",
            "synthetics:UntagResource",
            "tag:GetResources",
            "tag:TagResources",
            "tag:UntagResources",
            "transfer:TagResource",
            "transfer:UntagResource",
            "waf-regional:TagResource",
            "waf-regional:UntagResource",
            "waf:TagResource",
            "waf:UntagResource",
            "wafv2:TagResource",
            "wafv2:UntagResource",
            "worklink:TagResource",
            "worklink:UntagResource",
            "workmail:TagResource",
            "workmail:UntagResource",
            "workspaces:CreateTags",
            "workspaces:DeleteTags",
            "xray:TagResource",
            "xray:UntagResource",
            "kinesisvideo:TagResource",
            "kinesisvideo:UntagResource",
            "redshift-serverless:TagResource",
            "redshift-serverless:UntagResource",
            "route53-recovery-control-config:TagResource",
            "route53-recovery-control-config:UntagResource",
            "route53-recovery-readiness:TagResource",
            "route53-recovery-readiness:UntagResource",
            "ssm-contacts:TagResource",
            "ssm-contacts:UntagResource",
            "ssm-incidents:TagResource",
```

```
        "ssm-incidents:UntagResource",
        "vpc-lattice:TagResource",
        "vpc-lattice:UntagResource",
        "workspaces-web:TagResource",
        "workspaces-web:UntagResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAAmazonEBSCSIDriverOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Amazon EBS Container Storage Interface (CSI) Driver Operator, den Amazon EBS CSI-Treiber auf einem Red Hat OpenShift Service on AWS (ROSA) - Cluster zu installieren und zu warten. Der Amazon EBS CSI-Treiber ermöglicht es ROSA-Clustern, den Lebenszyklus von Amazon EBS-Volumes für persistente Volumes zu verwalten.

`ROSAAmazonEBSCSIDriverOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAAmazonEBSCSIDriverOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:36 UTC
- Bearbeitete Zeit: 22. Januar 2025, 00:52 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/ROSAAmazonEBSCSIDriverOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVolume",
        "ec2:ModifyVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVolumeFromSnapshot",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVolume"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "CreateSnapshotResourceTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSnapshotRequestTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSnapshot"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVolume",
            "CreateSnapshot"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSACloudNetworkConfigOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Cloud Network Config Controller Operator die Bereitstellung und Verwaltung von Netzwerkressourcen für die Nutzung durch das Red Hat OpenShift Service on AWS (ROSA) Cluster-Netzwerk-Overlay. Der OpenShift Cloud Network Operator stellt im Namen AWS APIs der Netzwerk-Plugins über CustomResourceDefinitions eine Verbindung her. Der Betreiber verwendet diese Richtlinienberechtigungen, um private IP-Adressen für EC2 Amazon-Instances als Teil des ROSA-Clusters zu verwalten.

`ROSACloudNetworkConfigOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSACloudNetworkConfigOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:34 UTC
- Bearbeitete Zeit: 20. April 2023, 22:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSACloudNetworkConfigOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DescribeNetworkResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "ModifyEIPs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignIpv6Addresses",
        "ec2:AssignIpv6Addresses"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAControlPlaneOperatorPolicy

Beschreibung: Ermöglicht der Red Hat OpenShift Service on AWS (ROSA) -Steuerebene die Verwaltung der ROSA-Cluster-Amazon EC2 - und Amazon Route 53-Ressourcen.

`ROSAControlPlaneOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAControlPlaneOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 24. April 2023, 23:02 UTC
- Bearbeitete Zeit: 10. April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAControlPlaneOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "route53:ListHostedZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
```

```
      ]
    },
    {
      "Sid" : "ListResourceRecordSets",
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local"
          ]
        }
      }
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAImageRegistryOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Image Registry Operator die Bereitstellung und Verwaltung von Amazon S3 S3-Buckets und Objekten zur Verwendung durch die Cluster-Image-Registry Red Hat OpenShift Service on AWS (ROSA), um die ROSA-Speicheranforderungen zu erfüllen. Der OpenShift Image Registry Operator installiert und verwaltet die interne Registrierung eines Red Hat OpenShift Clusters.

`ROSAImageRegistryOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAImageRegistryOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:13 UTC
- Bearbeitete Zeit: 19. Mai 2025, 18:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAImageRegistryOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ListBuckets",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSpecificBucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}"
      ]
    },
    {
      "Sid" : "AllowSpecificObjectActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}-*/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}?/*",
        "arn:aws:s3:::*-image-registry-${aws:RequestedRegion}/*"
      ]
    }
```

```
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAIngressOperatorPolicy

Beschreibung: Ermöglicht dem OpenShift Ingress Operator die Bereitstellung und Verwaltung von Load Balancers und DNS-Konfigurationen (Domain Name System) für Red Hat OpenShift Service on AWS (ROSA) -Cluster. Die Richtlinie ermöglicht den Lesezugriff auf Tag-Werte, die der Operator nach Route 53 53-Ressourcen filtert, um gehostete Zonen zu erkennen.

`ROSAIngressOperatorPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAIngressOperatorPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:37 UTC
- Bearbeitete Zeit: 10. April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAIngressOperatorPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeLoadBalancers",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAInstallerPolicy

Beschreibung: Ermöglicht dem Red Hat OpenShift Service on AWS (ROSA) -Installationsprogramm die Verwaltung von AWS Ressourcen, die die ROSA-Clusterinstallation unterstützen. Dies beinhaltet die Verwaltung von Instanzprofilen für ROSA-Worker-Knoten.

`ROSAInstallerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAInstallerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 6. Juni 2023, 21:00 Uhr UTC
- Bearbeitete Zeit: 11. August 2025, 17:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAInstallerPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeRegions",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeCapacityReservations",
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeLoadBalancers",
        "iam:GetOpenIDConnectProvider",
        "iam:GetRole",
        "route53:GetHostedZone",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets",
        "route53:GetAccountLimit",
        "servicequotas:GetServiceQuota"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToEC2",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "ManageInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:GetInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ]
    },
    {
      "Sid" : "CreateInstanceProfiles",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateInstanceProfile",
        "iam:TagInstanceProfile"
      ],
      "Resource" : [
        "arn:aws:iam::*:instance-profile/rosa-service-managed-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "GetSecretValue",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "Route53ManageRecords",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.hypershift.local",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "Route53Manage",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource",
        "route53:CreateHostedZone",
        "route53:DeleteHostedZone"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:snapshot/*"
      ]
    },
    {
      "Sid" : "RunInstancesRestrictedRequestTag",
      "Effect" : "Allow",
      "Action" : "ec2:RunInstances",
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRedHatOwnedAMIs",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
```

```
            "251351625822",
            "210686502322"
          ]
        }
      }
    },
    {
      "Sid" : "ManageInstancesRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances",
        "ec2:GetConsoleOutput"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateSecurityGroup"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "DeleteTagsK8sSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "kubernetes.io/cluster/*"
          ]
        }
      }
    },
    {
      "Sid" : "ListPoliciesAttachedToRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAKMSProviderPolicy

Beschreibung: Ermöglicht dem integrierten ROSA AWS Encryption Provider die Verwaltung von AWS Key Management Service (KMS) -Schlüsseln zur Unterstützung der etcd-Datenverschlüsselung mit einem vom Kunden bereitgestellten AWS KMS-Schlüssel. Die Richtlinie ermöglicht die Verschlüsselung und Entschlüsselung von Daten mithilfe von KMS-Schlüsseln.

`ROSAKMSProviderPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAKMSProviderPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:10 UTC
- Bearbeitete Zeit: 27. April 2023, 20:10 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKMSProviderPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "VolumeEncryption",
      "Effect" : "Allow",
      "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAKubeControllerPolicy

Beschreibung: Ermöglicht dem ROSA Kubernetes-Controller die Verwaltung von Amazon- EC2, Elastic Load Balancing- (ELB) - und AWS Key Management Service (KMS) -Ressourcen für einen ROSA-Cluster.

`ROSAKubeControllerPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAKubeControllerPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. April 2023, 20:09 UTC
- Bearbeitete Zeit: 10. April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAKubeControllerPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeRouteTables",
```

```
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeLoadBalancerPolicies"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "KMSDescribeKey",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagement",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:AddTags",
        "elasticloadbalancing:ConfigureHealthCheck",
        "elasticloadbalancing:CreateLoadBalancerPolicy",
        "elasticloadbalancing:DeleteLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:ModifyLoadBalancerAttributes",
        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer"
      ],
      "Resource" : [
        "*"
```

```
      ]
    },
    {
      "Sid" : "CreateTargetGroup",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "LoadBalanacerManagementResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DeleteListener",
        "elasticloadbalancing:RegisterTargets",
        "elasticloadbalancing:ModifyTargetGroup",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ApplySecurityGroupsToLoadBalancer",
        "elasticloadbalancing:CreateLoadBalancerListeners",
        "elasticloadbalancing:DeleteLoadBalancerListeners",
        "elasticloadbalancing:AttachLoadBalancerToSubnets",
        "elasticloadbalancing:DetachLoadBalancerFromSubnets",
        "elasticloadbalancing:ModifyListener",
        "elasticloadbalancing:SetLoadBalancerPoliciesOfListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateListeners",
```

```
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateListener"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true",
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "CreateLoadBalancer",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:CreateLoadBalancer"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifySecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAManageSubscription

Beschreibung: Diese Richtlinie stellt die Berechtigungen bereit, die für die Verwaltung des Red Hat OpenShift Service On AWS (ROSA) -Abonnements erforderlich sind.

`ROSAManageSubscription`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAManageSubscription` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. April 2022, 20:58 UTC
- Bearbeitete Zeit: 4. August 2023, 19:59 UTC
- ARN: `arn:aws:iam::aws:policy/ROSAManageSubscription`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:Subscribe",
        "aws-marketplace:Unsubscribe"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws-marketplace:ProductId" : [
            "34850061-abaf-402d-92df-94325c9e947f",
            "bfdca560-2c78-4e64-8193-794c159e6d30"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSANodePoolManagementPolicy

Beschreibung: Ermöglicht Red Hat OpenShift Service on AWS (ROSA), EC2 Cluster-Instanzen als Worker-Knoten zu verwalten, einschließlich der Erlaubnis, Sicherheitsgruppen zu konfigurieren und Instanzen und Volumes zu kennzeichnen. Diese Richtlinie ermöglicht auch die Verwendung von EC2 Instanzen mit Festplattenverschlüsselung, die durch AWS Key Management Service (KMS) - Schlüssel bereitgestellt wird.

`ROSANodePoolManagementPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSANodePoolManagementPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 8. Juni 2023, 20:48 UTC
- Bearbeitete Zeit: 09. September 2025, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSANodePoolManagementPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "CreateServiceLinkedRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/aws-service-role/elasticloadbalancing.amazonaws.com/
AWSServiceRoleForElasticLoadBalancing"
      ],
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "elasticloadbalancing.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassWorkerRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:*:iam::*:role/*-ROSA-Worker-Role"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "AuthorizeSecurityGroupIngressRestrictedResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfaces",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "NetworkInterfacesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyNetworkInterfaceAttribute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
```

```
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "TerminateInstances",
      "Effect" : "Allow",
      "Action" : [
        "ec2:TerminateInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "RunInstances"
          ]
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileNetworkInterface",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTagsCAPAControllerReconcileVolume",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesRequest",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "RunInstancesNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:capacity-reservation/*"
      ]
    },
    {
      "Sid" : "RunInstancesRedHatAMI",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:image/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:Owner" : [
            "531415883065",
            "251351625822"
          ]
        }
      }
    },
    {
      "Sid" : "ManagedKMSRestrictedResourceTag",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:DescribeKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/red-hat" : "true"
        }
      }
    },
    {
      "Sid" : "CreateGrantRestricted",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : true
        },
        "StringEquals" : {
          "aws:ResourceTag/red-hat" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSASharedVPCEndpointPolicy

Beschreibung: Ermöglicht dem Red Hat OpenShift Service on AWS (ROSA) -Installationsprogramm die Konfiguration von VPC-Endpunkten und Sicherheitsgruppen. Vorgesehen für die Verwendung auf einer gemeinsam genutzten VPC.

`ROSASharedVPCEndpointPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSASharedVPCEndpointPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. August 2025, 17:19 Uhr UTC
- Zeit bearbeitet: 11. August 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCEndpointPolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "SecurityGroupIngressEgress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "CreateSecurityGroupsVPCNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "VPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "VPCEndpointResourceTagCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "VPCEndpointNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ]
    },
    {
      "Sid" : "ManageVPCEndpointWithCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyVPCEndpoingNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*"
      ]
    },
    {
      "Sid" : "CreateTagsRestrictedActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpcEndpoint",
            "CreateSecurityGroup"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSASharedVPCRoute53Policy

Beschreibung: Ermöglicht dem Red Hat OpenShift Service on AWS (ROSA) -Installationsprogramm die Konfiguration von Route53-Datensätzen. Vorgesehen für die Verwendung auf einer gemeinsam genutzten VPC.

`ROSASharedVPCRoute53Policy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSASharedVPCRoute53Policy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 11. August 2025, 17:19 Uhr UTC
- Zeit bearbeitet: 11. August 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/ROSASharedVPCRoute53Policy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
        "route53:ListResourceRecordSets",
        "route53:ListHostedZones",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ChangeResourceRecordSetsRestrictedRecordNames",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeResourceRecordSets"
      ],
      "Resource" : [
        "*"
```

```
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "route53:ChangeResourceRecordSetsNormalizedRecordNames" : [
            "*.hypershift.local",
            "*.openshiftapps.com",
            "*.devshift.org",
            "*.openshiftusgov.com",
            "*.devshiftusgov.com"
          ]
        }
      }
    },
    {
      "Sid" : "ChangeTagsForResourceNoCondition",
      "Effect" : "Allow",
      "Action" : [
        "route53:ChangeTagsForResource"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSASRESupportPolicy

Beschreibung: Bietet ROSA Site Reliability Engineering (SRE) die erforderlichen Berechtigungen für die anfängliche Beobachtung, Diagnose und Unterstützung von AWS Ressourcen im Zusammenhang mit Red Hat OpenShift Service on AWS (ROSA) -Clustern, einschließlich der Möglichkeit, den Status des ROSA-Clusterknotens zu ändern.

`ROSASRESupportPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSASRESupportPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 1. Juni 2023, 14:36 UTC
- Bearbeitete Zeit: 10. April 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSASRESupportPolicy`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions",
        "sts:DecodeAuthorizationMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Route53",
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHostedZone",
```

```
        "route53:GetHostedZoneCount",
        "route53:ListHostedZones",
        "route53:ListHostedZonesByName",
        "route53:ListResourceRecordSets"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DecribeIAMRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "EC2DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeScheduledInstances"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "VPCNetwork",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables"
      ],
      "Resource" : [
```

```
        "*"
      ]
    },
    {
      "Sid" : "Cloudtrail",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:DescribeTrails",
        "cloudtrail:LookupEvents"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "Cloudwatch",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVolumes",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumesModifications",
        "ec2:DescribeVolumeStatus"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeLoadBalancers",
      "Effect" : "Allow",
      "Action" : [
        "elasticloadbalancing:DescribeAccountLimits",
        "elasticloadbalancing:DescribeInstanceHealth",
```

```
        "elasticloadbalancing:DescribeListenerCertificates",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeRules",
        "elasticloadbalancing:DescribeSSLPolicies",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroupAttributes",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpoints"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeSecurityGroups",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeStaleSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAddressesAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeAddressesAttribute",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*"
```

```
    },
    {
      "Sid" : "DescribeInstance",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeSpotFleetInstances",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeSpotFleetInstances",
      "Resource" : "arn:aws:ec2:*:*:spot-fleet-request/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "DescribeVolumeAttribute",
      "Effect" : "Allow",
      "Action" : "ec2:DescribeVolumeAttribute",
      "Resource" : "arn:aws:ec2:*:*:volume/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    },
    {
      "Sid" : "ManageInstanceLifecycle",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RebootInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
```

```
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ROSAWorkerInstancePolicy

Beschreibung: Ermöglicht Red Hat OpenShift Service auf AWS (ROSA) Worker Nodes in Ihrem Konto Lesezugriff auf EC2 Amazon-Instances und AWS-Regionen für das Lifecycle Management von Rechenknoten.

`ROSAWorkerInstancePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ROSAWorkerInstancePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. April 2023, 22:35 UTC
- Bearbeitete Zeit: 20. März 2025, 23:07 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ROSAWorkerInstancePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "EC2DescribeInstancesRegions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRGetAuthorizationToken",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ECRReadOnlyAccessRedHatManaged",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer",
        "ecr:GetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:DescribeImages",
        "ecr:BatchGetImage",
        "ecr:ListTagsForResource"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/red-hat-managed" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Route53RecoveryReadinessServiceRolePolicy

Beschreibung: Service Linked Role Policy für Route 53 Recovery Readiness

`Route53RecoveryReadinessServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 15. Juli 2021, 16:06 UTC
- Bearbeitete Zeit: 14. Februar 2023, 18:08 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53RecoveryReadinessServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive"
      ],
      "Resource" : "arn:aws:dynamodb:*:*:table/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/servicequotas.amazonaws.com/
AWSServiceRoleForServiceQuotas",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    },
```

```
    {
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConcurrency",
        "lambda:GetFunctionConfiguration",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListVersionsByFunction"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBClusters"
      ],
      "Resource" : "arn:aws:rds:*:*:cluster:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "rds:DescribeDBInstances"
      ],
      "Resource" : "arn:aws:rds:*:*:db:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:ListResourceRecordSets"
      ],
      "Resource" : "arn:aws:route53:::hostedzone/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "route53:GetHealthCheck",
        "route53:GetHealthCheckStatus"
      ],
      "Resource" : "arn:aws:route53:::healthcheck/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "servicequotas:RequestServiceQuotaIncrease"
      ],
      "Resource" : "arn:aws:servicequotas:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sns:GetTopicAttributes",
        "sns:ListSubscriptionsByTopic"
      ],
      "Resource" : "arn:aws:sns:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl"
      ],
      "Resource" : "arn:aws:sqs:*:*:*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "autoscaling:DescribeAccountLimits",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeLifecycleHooks",
        "autoscaling:DescribeLoadBalancers",
        "autoscaling:DescribeLoadBalancerTargetGroups",
        "autoscaling:DescribeNotificationConfigurations",
        "autoscaling:DescribePolicies",
        "cloudwatch:GetMetricData",
        "cloudwatch:DescribeAlarms",
        "dynamodb:DescribeLimits",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeInstances",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetEbsDefaultKmsKeyId",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "kafka:DescribeCluster",
        "kafka:DescribeConfigurationRevision",
        "lambda:ListEventSourceMappings",
        "lambda:ListFunctions",
        "rds:DescribeAccountAttributes",
        "route53:GetHostedZone",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "sns:GetEndpointAttributes",
        "sns:GetSubscriptionAttributes"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Route53ResolverServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die von Route53 Resolver verwendeten oder verwalteten Ressourcen

`Route53ResolverServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 12. August 2020, 17:47 Uhr UTC
- Bearbeitete Zeit: 12. August 2020, 17:47 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/Route53ResolverServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups",
        "s3:GetBucketPolicy"
      ],
```

```
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

RTBFabricServiceRolePolicy

Beschreibung: Eine dienstbezogene Rolle, die für die AWS RTBFabric Erstellung und Verwaltung Ihrer Netzwerkschnittstellenressourcen und die Bereitstellung von Metriken erforderlich ist.

`RTBFabricServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. Oktober 2025, 16:49 UTC
- Zeit bearbeitet: 17. Oktober 2025, 19:19 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/RTBFabricServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "RTBFabricRoleCreateTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleCreateNetworkInterfacePermissionActions",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterfacePermission",
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
```

```
    {
      "Sid" : "RTBFabricRoleModifyTaggedNetworkInterfaceActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/RTBFabricManaged" : "true"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleTaggingActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CreateNetworkInterface"
        }
      }
    },
    {
      "Sid" : "RTBFabricRoleDescribeActions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RTBFabricRolePutMetricDataActions",
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/RTBFabric"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

S3StorageLensServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und die Ressourcen, die von S3 Storage Lens verwendet oder verwaltet werden

`S3StorageLensServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 18. November 2020, 18:15 Uhr UTC
- Zeit bearbeitet: 18. November 2020, 18:15 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/S3StorageLensServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrgsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioAdminIAMConsolePolicy

Beschreibung: Bietet anfängliche administrative und individuelle Einrichtungsrechte für Amazon SageMaker Unified Studio über das SDK AWS-Managementkonsole und. Ermöglicht das Starten des SageMaker Unified Studio-Portals.

`SageMakerStudioAdminIAMConsolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioAdminIAMConsolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 22:49 UTC
- Bearbeitete Zeit: 14. November 2025, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMConsolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
```

```
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*"
      ]
    },
    {
```

```
      "Sid" : "DescribeEc2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpc"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateSubnetInTaggedVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSubnet"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedSecurityGroupInVPC",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "CreateTaggedVPCEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateVPCEndpointInTaggedResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateInternetGateway"
      ],
      "Resource" : "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "CreateTaggedNatGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:natgateway/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateNatGatewayInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNatGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:elastic-ip/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateTaggedRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRouteTableInTaggedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRouteTable"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllocateAddress",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AllocateAddress"
      ],
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "ModifyTaggedEc2Resources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyVpcAttribute",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AttachInternetGateway",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachInternetGateway"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:internet-gateway/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "CreateRoute",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateRoute"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:route-table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AssociateRouteTable",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AssociateRouteTable"
      ],
      "Resource" : [
```

```
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TaggingOperations",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : [
            "CreateVpc",
            "CreateSubnet",
            "CreateSecurityGroup",
            "CreateInternetGateway",
            "CreateNatGateway",
            "CreateRouteTable",
            "CreateVpcEndpoint"
          ],
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "Ec2TagEIP",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:elastic-ip/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "AllowCFNStackCreation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:CreateStack",
        "cloudformation:GetTemplateSummary",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DeleteTaggedVpcResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteVpc",
        "ec2:DeleteSubnet",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteNatGateway",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteRouteTable",
        "ec2:DeleteRoute",
        "ec2:ReleaseAddress"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
      "Sid" : "DeleteTagsOnTaggedResources",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteTags",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:ResourceTag/CreatedForUseWithSageMakerUnifiedStudio" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "S3ReadCFNTemplate",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "KMSReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "DataZoneKMSGrantPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioAdminIAMDefaultExecutionPolicy

Beschreibung: Administrative Ausführungsrichtlinie für die Verwendung von IAM-Rollen mit SageMaker Unified Studio. Ermöglicht Administratoren die Bereitstellung, Verwaltung und den Zugriff auf Ressourcen in Ihrem Konto (mit Ausnahme des Zugriffs auf Datenressourcen) für die IAM-basierte Nutzung von Unified Studio. SageMaker

`SageMakerStudioAdminIAMDefaultExecutionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioAdminIAMDefaultExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 17:19 Uhr UTC
- Bearbeitete Zeit: 18. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMDefaultExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
```

```
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "datazone.amazonaws.com",
            "bedrock.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMParameter",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "ManageSageMakerSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:*",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*",
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:user-profile/*"
      ]
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
```

```
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:Batch*",
        "sagemaker:DeleteTags",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:Get*",
        "s3:Put*"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "S3List",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:connection/*"
      ]
    },
```

```
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:Describe*",
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:UseGlueStudio",
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
```

```
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
```

```
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
```

```
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManageScheduler",
      "Effect" : "Allow",
      "Action" : "scheduler:*",
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsAdmin",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioAdminIAMPermissiveExecutionPolicy

Beschreibung: Administrative Ausführungsrichtlinie für die Verwendung von IAM-Rollen mit SageMaker Unified Studio. Ermöglicht Administratoren die Bereitstellung, Verwaltung und den Zugriff auf Ressourcen im lokalen Konto (einschließlich umfassendem Zugriff auf APIs All-In-Datendienste wie S3, Glue, CloudWatch Logs und andere) für die IAM-basierte Nutzung von SageMaker Unified Studio.

`SageMakerStudioAdminIAMPermissiveExecutionPolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioAdminIAMPermissiveExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 17:19 Uhr UTC
- Bearbeitete Zeit: 18. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminIAMPermissiveExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "datazone:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
```

```
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:GetUser",
        "iam:ListUsers",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
```

```
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless",
        "arn:aws:iam::*:role/aws-service-role/ops.athena.amazonaws.com/
AWSServiceRoleForAmazonAthena"
      ]
    },
    {
      "Sid" : "TagRoleAndSession",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "sts:TagSession"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForProvisioning",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "athena.amazonaws.com",
            "glue.amazonaws.com",
            "datazone.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
        "arn:aws:iam::*:role/${aws:PrincipalTag/AmazonDataZonePassedRolePath}"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "datazone.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CreateRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ]
    },
    {
```

```
      "Sid" : "AttachPolicy",
      "Effect" : "Allow",
      "Action" : "iam:AttachRolePolicy",
      "Resource" : "arn:aws:iam::*:role/service-role/AmazonSageMaker*",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteParameter",
        "ssm:GetParameter*",
        "ssm:PutParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
```

```
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DeregisterResource",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions",
        "lakeformation:ListLakeFormationOptIns",
        "lakeformation:CreateLakeFormationOptIn",
        "lakeformation:DeleteLakeFormationOptIn"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ManagePrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:TagResource",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*"
    },
    {
      "Sid" : "Ecr",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnections",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:*",
        "codestar-connections:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
```

```
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ]
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "SGCreateTags",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
```

```
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioAdminProjectUserRolePolicy

Beschreibung: Diese IAM-Richtlinie gewährt einer IAM-Rolle vollen Zugriff auf AWS Glue Data Catalog (Metadaten) und Amazon S3 (tatsächliche Daten) für Data Lake-Operationen, wobei der Zugriff auf Konten und Rollen-Tags beschränkt ist.

`SageMakerStudioAdminProjectUserRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioAdminProjectUserRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Juli 2025, 20:52 UTC
- Bearbeitete Zeit: 10. Juli 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
```

```
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    },
```

```
    {
      "Sid" : "DataAccessPermissionsForS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aws:PrincipalTag/BootstrappedServices" : "*glue*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockAgentServiceRolePolicy

Beschreibung: Ermöglicht Amazon Bedrock Agents den Zugriff auf Amazon Bedrock-Modelle und andere Ressourcen, die mit einem Agenten in SageMaker Studio verknüpft sind.

`SageMakerStudioBedrockAgentServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockAgentServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 13. Februar 2025, 23:37 UTC
- Bearbeitete Zeit: 13. Februar 2025, 23:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockAgentServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockApplyGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
```

```
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockRetrievePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3GetObjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAttributes",
        "s3:GetObjectAttributes"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
```

```
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockChatAgentUserRolePolicy

Beschreibung: Bietet Zugriff auf die Konfiguration einer Amazon Bedrock Chat-Agent-App und auf den Amazon Bedrock-Agenten in SageMaker Studio.

`SageMakerStudioBedrockChatAgentUserRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockChatAgentUserRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 13. Februar 2025, 23:52 UTC
- Zeit bearbeitet: 13. Februar 2025, 23:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockChatAgentUserRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
```

```
      "Sid" : "BedrockGetAgentAliasPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetAgentAlias",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/${aws:PrincipalTag/AgentId}/
${aws:PrincipalTag/AgentAliasId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGetAndListAgentMetadataPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions"
      ],
      "Resource" : "arn:aws:bedrock:*:*:agent/${aws:PrincipalTag/AgentId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/AppDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetAppDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AppDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AppDefinitionPath" : ""
        }
```

```
      }
    },
    {
      "Sid" : "S3ListDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/DataSourcePath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/DataSourcePath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/DataSourcePath" : ""
        }
      }
    },
    {
```

```
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/${aws:PrincipalTag/AgentId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockEvaluationJobServiceRolePolicy

Beschreibung: Ermöglicht Amazon Bedrock den Zugriff auf Amazon Bedrock-Modelle und -Datensätze für Bewertungsaufgaben in Studio. SageMaker

`SageMakerStudioBedrockEvaluationJobServiceRolePolicy`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockEvaluationJobServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Februar 2025, 00:37 UTC
- Zeit bearbeitet: 14. Februar 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockEvaluationJobServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockEvaluationInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateModelInvocationJob",
        "bedrock:StopModelInvocationJob",
        "bedrock:GetProvisionedModelThroughput"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3GetBucketLocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketLocation",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        }
      }
    },
    {
      "Sid" : "S3ListBucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
        },
        "StringNotEquals" : {
```

```
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "S3EvaluationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/${aws:PrincipalTag/
AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "KmsDescribeKeyPermissions",
      "Effect" : "Allow",
      "Action" : "kms:DescribeKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockFlowServiceRolePolicy

Beschreibung: Ermöglicht Amazon Bedrock Flows den Zugriff auf Amazon Bedrock-Modelle und andere Ressourcen, die an einen Flow in SageMaker Studio angehängt sind.

`SageMakerStudioBedrockFlowServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockFlowServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Februar 2025, 00:07 Uhr UTC
- Zeit bearbeitet: 09. April 2025, 20:37 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFlowServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
      "Resource" : "arn:aws:bedrock:*:*:prompt/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:Retrieve",
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ApplyGuardrail",
      "Resource" : "arn:aws:bedrock:*:*:guardrail/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowLambdaInvokeFunctionInProjectPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "AllowBedrockApplicationInferenceProfileAccessInProjectPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowBedrockInvokeModelAccessWithInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeModel",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeAgent",
      "Resource" : "arn:aws:bedrock:*:*:agent-alias/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockGuardrailKmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:guardrail-id" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockAgentKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:agent/*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockFunctionExecutionRolePolicy

Beschreibung: Ermöglicht AWS Lambda den Zugriff auf die Konfiguration einer Amazon Bedrock-Funktionskomponente in SageMaker Studio.

`SageMakerStudioBedrockFunctionExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockFunctionExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. Februar 2025, 03:52 UTC

- Bearbeitete Zeit: 25. Februar 2025, 03:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockFunctionExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SecretsManagerReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "KMSSameAccountBedrockViaSecretsManagerPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "secretsmanager.*.amazonaws.com",
          "kms:EncryptionContext:SecretARN" : "arn:aws:secretsmanager:*:
${aws:PrincipalAccount}:secret:amazon-bedrock*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy

Beschreibung: Bietet Zugriff auf die Konfiguration von Vektorspeichern und Amazon Bedrock-Wissensdatenbanken in SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. Februar 2025, 03:37 UTC
- Bearbeitete Zeit: 25. Februar 2025, 03:37 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob"
      ],
      "Resource" : "arn:aws:bedrock:*:*:knowledge-base/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy

Beschreibung: Ermöglicht Amazon Bedrock Knowledge Bases den Zugriff auf Amazon Bedrock-Modelle und -Datenquellen in SageMaker Studio.

`SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 25. Februar 2025, 02:52 UTC
- Bearbeitete Zeit: 15. Juli 2025, 17:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermission",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
```

```
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
    {
      "Sid" : "OpenSearchServerlessPermissions",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "arn:aws:aoss:*:*:collection/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "aoss:collection" : "bedrock*"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
```

```
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "VectorStoresKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "VectorStoresKmsDescribeKey",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "NeptuneGraphDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:GetGraph",
        "neptune-graph:DeleteDataViaQuery",
        "neptune-graph:WriteDataViaQuery",
        "neptune-graph:ReadDataViaQuery"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3VectorsDataAccess",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:GetVectorBucket",
        "s3vectors:GetIndex",
        "s3vectors:PutVectors",
        "s3vectors:GetVectors",
        "s3vectors:ListVectors",
```

```
        "s3vectors:QueryVectors",
        "s3vectors:DeleteVectors"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-${aws:PrincipalTag/
AmazonDataZoneProject}*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:knowledge-base/*"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
```

```
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "SqlWorkbenchAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:GetSqlRecommendations",
        "sqlworkbench:PutSqlGenerationContext",
        "sqlworkbench:GetSqlGenerationContext",
        "sqlworkbench:DeleteSqlGenerationContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockGenerateQueryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GenerateQuery"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioBedrockPromptUserRolePolicy

Beschreibung: Ermöglicht den Zugriff auf eine Amazon Bedrock-Eingabeaufforderung und deren Konfiguration in SageMaker Studio.

`SageMakerStudioBedrockPromptUserRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioBedrockPromptUserRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 14. Februar 2025, 00:22 UTC
- Zeit bearbeitet: 14. Februar 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioBedrockPromptUserRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BedrockPromptReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:GetPrompt",
```

```
      "Resource" : "arn:aws:bedrock:*:*:prompt/${aws:PrincipalTag/PromptId}:
${aws:PrincipalTag/PromptVersion}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "S3ListPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "s3:prefix" : "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/${aws:PrincipalTag/PromptDefinitionPath}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "S3GetPromptDefinitionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/PromptDefinitionPath}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringNotEquals" : {
```

```
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/PromptDefinitionPath" : ""
        }
      }
    },
    {
      "Sid" : "BedrockPromptKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com",
          "kms:EncryptionContext:aws:bedrock-prompts:arn" : "arn:aws:bedrock:*:
${aws:PrincipalAccount}:prompt/${aws:PrincipalTag/PromptId}"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3KmsPermissions",
      "Effect" : "Allow",
      "Action" : "kms:Decrypt",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioDomainExecutionRolePolicy

Beschreibung: Diese Richtlinie wird von Amazon SageMaker Studio verwendet, um Daten in der Amazon SageMaker Studio-Domain zu katalogisieren, zu ermitteln, zu verwalten, zu teilen und zu analysieren.

`SageMakerStudioDomainExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioDomainExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. November 2024, 21:56 UTC
- Bearbeitete Zeit: 18. November 2025, 21:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:AddEntityOwner",
        "datazone:AddPolicyGrant",
        "datazone:AssociateGovernedTerms",
        "datazone:BatchGetAttributesMetadata",
        "datazone:BatchPutAttributesMetadata",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetFilter",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateConnection",
        "datazone:CreateDataProduct",
        "datazone:CreateDataProductRevision",
        "datazone:CreateDataSource",
        "datazone:CreateDomainUnit",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateRule",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
```

```
        "datazone:DeleteAsset",
        "datazone:DeleteAssetFilter",
        "datazone:DeleteAssetType",
        "datazone:DeleteConnection",
        "datazone:DeleteDataProduct",
        "datazone:DeleteDataSource",
        "datazone:DeleteDomainUnit",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteRule",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:DeleteTimeSeriesDataPoints",
        "datazone:DisassociateGovernedTerms",
        "datazone:GetAsset",
        "datazone:GetAssetFilter",
        "datazone:GetAssetType",
        "datazone:GetConnection",
        "datazone:GetDataProduct",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetDomainUnit",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentAction",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetLineageNode",
        "datazone:GetListing",
        "datazone:GetMetadataGenerationRun",
```

```
        "datazone:GetProject",
        "datazone:GetRule",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetTimeSeriesDataPoint",
        "datazone:GetUpdateEligibility",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetFilters",
        "datazone:ListAssetRevisions",
        "datazone:ListConnections",
        "datazone:ListDataProductRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListDomainUnitsForParent",
        "datazone:ListEntityOwners",
        "datazone:ListEnvironmentActions",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListLineageNodeHistory",
        "datazone:ListMetadataGenerationRuns",
        "datazone:ListNotifications",
        "datazone:ListPolicyGrants",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListRules",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListTimeSeriesDataPoints",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RemoveEntityOwner",
        "datazone:RemovePolicyGrant",
```

```
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateDataSource",
        "datazone:UpdateDomainUnit",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateRule",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RAMResourceShareStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShareAssociations",
        "ram:GetResourceShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage",
        "q:ListConversations",
        "q:GetConversation",
        "q:PassRequest",
        "q:GetIdentityMetadata",
```

```
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSetTrustedIdentity",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : "arn:aws:sts::*:self"
    },
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q/${aws:PrincipalTag/datazone-
domainId}*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/${aws:PrincipalTag/datazone-
domainId}/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
```

```
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ListCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codestar-connections:ListConnections",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "UseCodeConnectionsPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codestar-connections:UseConnection"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "ProjectProfilePermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetProjectProfile",
        "datazone:ListProjectProfiles"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    },
    {
```

```
      "Sid" : "AccountPoolPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:GetAccountPool",
        "datazone:ListAccountPools",
        "datazone:ListAccountsInAccountPool"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioDomainServiceRolePolicy

Beschreibung: Servicerolle für Aktionen auf Domainebene im Portal, die von Amazon SageMaker Studio ausgeführt werden.

`SageMakerStudioDomainServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioDomainServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. November 2024, 21:56 UTC
- Bearbeitete Zeit: 20. November 2024, 21:56 UTC

- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioDomainServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMGetParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles/*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
```

```
          "kms:ViaService" : "ssm.*.amazonaws.com",
          "kms:EncryptionContext:PARAMETER_ARN" : "arn:aws:ssm:*:*:parameter/amazon/
datazone/profiles*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioEMRContainersSystemNamespaceRolePolicy

Beschreibung: Amazon SageMaker Studio erstellt IAM-Rollen für Projektbenutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Berechtigungen für EMR zu definieren.

`SageMakerStudioEMRContainersSystemNamespaceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioEMRContainersSystemNamespaceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 23. Oktober 2025, 18:34 UTC
- Bearbeitete Zeit: 30. Oktober 2025, 20:34 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRContainersSystemNamespaceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AssumeProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "TagSessionProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:TagSession"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
```

```
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/LakeFormationAuthorizedCaller" : "EMR on EKS Engine",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SetContextProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioEMRInstanceRolePolicy

Beschreibung: Amazon SageMaker Studio erstellt IAM-Rollen für Projektbenutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Berechtigungen für EMR zu definieren.

`SageMakerStudioEMRInstanceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioEMRInstanceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 27. Februar 2025, 00:22 UTC
- Zeit bearbeitet: 27. Februar 2025, 00:22 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRInstanceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "AccessCertificateLocationS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessPatchingRPMsS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessBootstrapActionScriptS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/bootstrap-script/*",
```

```
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRClusterLogUploadS3Permission",
      "Effect" : "Allow",
      "Action" : "s3:PutObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
${aws:PrincipalTag/AmazonDataZoneScopeName}/sys/emr/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneScopeName" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EMRRuntimeRoleAssumePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "LakeFormationAuthorizedCaller"
          ]
        },
        "StringEquals" : {
          "iam:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioEMRServiceRolePolicy

Beschreibung: Amazon SageMaker Studio erstellt IAM-Rollen für Projektbenutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Berechtigungen für EMR zu definieren.

`SageMakerStudioEMRServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioEMRServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 31. Januar 2025, 19:52 UTC
- Bearbeitete Zeit: 22. Juli 2025, 16:52 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "PassRoleToEMREC2InstanceRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_
${aws:PrincipalTag/AmazonDataZoneProject}_${aws:PrincipalTag/
AmazonDataZoneEnvironment}",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "",
          "aws:PrincipalTag/AmazonDataZoneEnvironment" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CreateInNetworkForSharedSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:RunInstances",
```

```
        "ec2:CreateFleet"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "EMRKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "ec2.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "AllowDescribeKeyForLogPusherCMK",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioFullAccess

Beschreibung: Diese Richtlinie bietet vollen Zugriff auf Amazon SageMaker Unified Studio über die Amazon SageMaker Management Console.

`SageMakerStudioFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 28. November 2024, 00:06 Uhr UTC
- Bearbeitete Zeit: 23. Juli 2025, 19:22 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioFullAccess`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:*"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListPolicies",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets",
        "iam:ListUsers",
        "glue:GetDatabases",
        "codeconnections:ListConnections",
        "codeconnections:ListTagsForResource",
        "codewhisperer:ListProfiles",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListFoundationModels",
        "bedrock:ListTagsForResource",
        "aoss:ListSecurityPolicies",
        "quicksight:DescribeAccountSubscription",
        "cloudformation:ValidateTemplate"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "BucketReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::*"
    },
    {
      "Sid" : "ReadManagedBlueprintTemplatesStatement",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : [
        "arn:aws:s3:::default-env-blueprint-*/*",
        "arn:aws:s3:*:*:accesspoint/env-blueprint-accesspoint*"
      ],
      "Condition" : {
        "ArnLike" : {
          "s3:DataAccessPointArn" : "arn:aws:s3:*:*:accesspoint/env-blueprint-
accesspoint"
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "CreateBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-datazone*",
        "arn:aws:s3:::amazon-sagemaker*"
      ]
    },
    {
      "Sid" : "ConfigureBucketStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutBucketCORS",
        "s3:PutBucketPolicy",
        "s3:PutBucketVersioning"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PutObjectStatement",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "RamCreateResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : "datazone:Domain"
        }
      }
    },
    {
      "Sid" : "RamResourceStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "RamResourceReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations",
        "ram:ListResourceSharePermissions"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "RamAssociateResourceSharePermissionStatement",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ram:PermissionArn" : [
            "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionAmazonDataZoneDomain",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionAmazonDataZoneDomainFullAccessWithPortalAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceAccess",
            "arn:aws:ram::aws:permission/
AWSRAMPermissionsAmazonDatazoneDomainExtendedServiceWithPortalAccess"
          ]
        }
      }
    },
    {
      "Sid" : "IAMPassRoleStatement",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:passedToService" : "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "IAMGetPolicyStatement",
      "Effect" : "Allow",
      "Action" : "iam:GetPolicy",
      "Resource" : [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
```

```
      "Sid" : "DataZoneTagOnCreateDomainProjectTags",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "DataZoneTagOnCreate",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*",
          "aws:ResourceTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "CreateSecretStatement",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret"
      ],
```

```
      "Resource" : "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/AmazonDataZoneDomain" : "dzd*"
        }
      }
    },
    {
      "Sid" : "ConnectionStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:GetConnection"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*"
      ]
    },
    {
      "Sid" : "TagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:TagResource"
      ],
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "for-use-with-all-datazone-projects"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "UntagCodeConnectionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UntagResource"
      ],
```

```
      "Resource" : [
        "arn:aws:codeconnections:*:*:connection/*",
        "arn:aws:codeconnections:*:*:host/*"
      ],
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : "for-use-with-all-datazone-projects"
        }
      }
    },
    {
      "Sid" : "SSMParameterStatement",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParametersByPath",
        "ssm:PutParameter",
        "ssm:DeleteParameter"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/profiles*"
      ]
    },
    {
      "Sid" : "UseKMSKeyPermissionsStatement",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "true"
        },
        "Null" : {
          "aws:ResourceTag/EnableKeyForAmazonDataZone" : "false"
        },
        "StringLike" : {
          "kms:ViaService" : "ssm.*.amazonaws.com"
        }
```

```
      }
    },
    {
      "Sid" : "SecurityPolicyStatement",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "aoss:collection" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "GetFoundationModelStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*"
      ]
    },
    {
      "Sid" : "GetInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:inference-profile/*",
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ]
    },
    {
      "Sid" : "ApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
```

```
        "bedrock:CreateInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "TagApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:TagResource"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false",
          "aws:RequestTag/AmazonDataZoneDomain" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteApplicationInferenceProfileStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:DeleteInferenceProfile"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:application-inference-profile/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "true",
          "aws:ResourceTag/AmazonDataZoneDomain" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ModelAccessUseCaseStatement",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetUseCaseForModelAccess",
        "bedrock:PutUseCaseForModelAccess"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioProjectProvisioningRolePolicy

Beschreibung: Amazon SageMaker Studio verwendet diese Richtlinie, um Ressourcen in Ihrem Konto bereitzustellen und zu verwalten.

`SageMakerStudioProjectProvisioningRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioProjectProvisioningRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen

- Erstellungszeit: 20. November 2024, 21:58 Uhr UTC
- Bearbeitete Zeit: 21. November 2025, 00:04 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioProjectProvisioningRolePolicy`

Version der Richtlinie

Richtlinienversion: v24 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CfnCreate",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:TagResource"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:UpdateStack"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CfnDelete",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "LFManage",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:PutDataLakeSettings",
        "lakeformation:RevokePermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:RegisterResource",
        "lakeformation:DeregisterResource",
        "lakeformation:GrantPermissions",
        "lakeformation:BatchGrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:DescribeResource",
        "lakeformation:*LakeFormationIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DzTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringEquals" : {
          "aws:CalledViaFirst" : "cloudformation.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DzCfTemplate",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::amazon-sagemaker-cf-templates*/*"
    },
    {
      "Sid" : "CcCreate",
      "Effect" : "Allow",
      "Action" : [
```

```
        "codecommit:CreateRepository",
        "codecommit:TagResource"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CcDelete",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:DeleteRepository",
        "codecommit:UntagResource",
        "codecommit:UpdateRepositoryEncryptionKey",
        "codecommit:PutRepositoryTriggers"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CcAccess",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:GetBranch",
        "codecommit:CreateCommit",
```

```
        "codecommit:GetRepository",
        "codecommit:GetFile"
      ],
      "Resource" : "arn:aws:codecommit:*:*:datazone*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CcList",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:ListRepositories"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CcKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "GetIamRole",
```

```
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ]
    },
    {
      "Sid" : "IAMManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrockExecution*",
        "arn:aws:iam::*:role/BedrockStudio*",
        "arn:aws:iam::*:role/AmazonBedrockConsumptionRole*",
        "arn:aws:iam::*:role/AmazonBedrockEvaluation*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamDzManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRolePolicy",
        "iam:PutRolePolicy"
      ],
```

```
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
```

```
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy",
            "arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRContainersSystemNamespaceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/SageMakerStudioEMRServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioEMRInstanceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/AmazonEMRServicePolicy_v2",
            "arn:aws:iam::aws:policy/service-role/
AmazonS3TablesLakeFormationServiceRole",
            "arn:aws:iam::aws:policy/AmazonSageMakerPartnerAppsFullAccess",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamManageAdmin",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneAdminProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/SageMakerStudioAdminProjectUserRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamManageBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy",
```

```
        "iam:DetachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockAgentServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockChatAgentUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFlowServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockFunctionExecutionRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseServiceRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockKnowledgeBaseCustomResourcePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockPromptUserRolePolicy",
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioBedrockEvaluationJobServiceRolePolicy"
          ]
        }
      }
    },
    {
      "Sid" : "IamTag",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/datazone_redshift_serverless_admin_role_*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*",
```

```
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "BootstrappedServices",
            "AmazonBedrockManaged",
            "RedshiftDb*",
            "EnableAmazonBedrockPermissions",
            "EnableAmazonBedrockIDEPermissions",
            "EnableGlueWorkloadsPermissions",
            "EnableSageMakerMLWorkloadsPermissions",
            "DomainBucketName",
            "KmsKeyId",
            "DomainKmsKeyId",
            "DefaultGlueCatalogKmsKeyId",
            "LogGroupName",
            "RoleName",
            "vpcArn",
            "VpcId",
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "AdminProjectTagRoleManagement",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZoneScopeName",
            "BootstrappedServices",
            "AmazonDataZoneAdminProject"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagBR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : "arn:aws:iam::*:role/AmazonBedrock*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "DomainBucketName",
            "KmsKeyId",
            "AgentId",
            "AgentAliasId",
            "AppDefinitionPath",
            "DataSourcePath",
            "PromptId",
            "PromptVersion",
            "PromptDefinitionPath",
            "OpenSearchServerlessCollectionId"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagRS",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
```

```
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "RedshiftDb*"
          ]
        }
      }
    },
    {
      "Sid" : "IamTagEMR",
      "Effect" : "Allow",
      "Action" : [
        "iam:TagRole",
        "iam:UntagRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*",
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*",
        "arn:aws:iam::*:role/datazone_emr_containers_system_namespace_role_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "DataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "DomainBucketName",
            "KmsKeyId",
            "VpcId"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "IamUntag",
      "Effect" : "Allow",
      "Action" : "iam:UntagRole",
      "Resource" : "arn:aws:iam::*:role/datazone_usr_role_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "EnableAmazonBedrockIDEPermissions"
        }
      }
    },
    {
      "Sid" : "ManageRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DzManageRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
```

```
        "arn:aws:iam::*:role/datazone_emr_*",
        "arn:aws:iam::*:role/datazone-partner-apps-*",
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IamAttach",
      "Effect" : "Allow",
      "Action" : [
        "iam:AttachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "IamDetach",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*",
        "arn:aws:iam::*:role/AmazonBedrock*"
      ]
    },
    {
      "Sid" : "DzManagePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DeletePolicy",
        "iam:CreatePolicy",
```

```
        "iam:ListPolicies",
        "iam:GetPolicy",
        "iam:GetPolicyVersion",
        "iam:CreatePolicyVersion",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource" : [
        "arn:aws:iam::*:policy/datazone*",
        "arn:aws:iam::*:policy/connector-manage-access-policy*",
        "arn:aws:iam::*:policy/SageMakerStudioQueryExecutionRolePolicy"
      ]
    },
    {
      "Sid" : "ListPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListPolicies"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType",
        "glue:*GlueIdentityCenterConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InstanceProfile",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetInstanceProfile",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
```

```
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaFirst" : [
            "cloudformation.amazonaws.com",
            "glue.amazonaws.com"
          ],
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForDZ",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForGlue",
```

```
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*",
        "arn:aws:iam::*:role/datazone_s3tables_*",
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmr",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_service_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "elasticmapreduce.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "PassRoleForEmrIP",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_emr_ec2_instance_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "ec2.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "PassRoleToBR",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PassRoleToLambda",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrock*",
        "arn:aws:iam::*:role/BedrockStudio*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AossSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/
observability.aoss.amazonaws.com/AWSServiceRoleForAmazonOpenSearchServerless",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "observability.aoss.amazonaws.com"
        }
      }
    },
    {
```

```
      "Sid" : "GlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/default",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog",
        "arn:aws:glue:*:*:catalog/s3tablescatalog/*",
        "arn:aws:glue:*:*:database/s3tablescatalog/*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CfnGlueDb",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueDbDelete",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteDatabase"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "GlueConnTag",
      "Effect" : "Allow",
      "Action" : "glue:GetConnection",
```

```
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnManage",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection",
        "glue:DeleteConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/datazone-glue-network-connection-*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueConnections",
      "Action" : [
        "glue:PassConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "AthenaConnection",
      "Action" : [
        "athena:CreateDataCatalog"
      ],
      "Resource" : "*",
      "Effect" : "Allow",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GetConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "ConnectionTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "federated_athena*"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CreateConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageConnection",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageCatalogConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteConnection",
```

```
        "glue:UpdateConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "GetDataCatalogEncSett",
      "Action" : "glue:GetDataCatalogEncryptionSettings",
      "Effect" : "Allow",
      "Resource" : "arn:aws:glue:*:*:catalog",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
```

```
      "Sid" : "Repo",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:GetCloudFormationTemplate",
        "serverlessrepo:CreateCloudFormationTemplate"
      ],
      "Resource" : [
        "arn:aws:serverlessrepo:*:*:applications/Athena*"
      ]
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "imagebuilder:GetComponent",
        "imagebuilder:GetContainerRecipe",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : [
        "arn:aws:ecr:*:*:repository/athena-federation-repository*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "lambda.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "CfnChangeSet",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:transform/Serverless*"
      ]
    },
    {
      "Sid" : "LambdaManage",
      "Effect" : "Allow",
```

```
      "Action" : [
        "lambda:CreateFunction",
        "lambda:DeleteFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "LambdaGet",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : [
            "athena.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaUpdate",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:TagResource"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:athenafederatedcatalog*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "aws:cloudformation:*",
            "federated_athena*",
            "lambda:createdBy"
          ]
        }
      }
    },
    {
      "Sid" : "LambdaS3Get",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:::awsserverlessrepo*"
      ],
      "Condition" : {
        "StringLike" : {
          "aws:CalledViaLast" : [
            "lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "s3:prefix" : "true"
        }
      }
    },
    {
      "Sid" : "S3Create",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutBucketCORS",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketPolicy",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy"
      ],
      "Resource" : [
        "arn:aws:s3:::sagemaker-*"
      ]
```

```
    },
    {
      "Sid" : "Cfn",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/athenafederatedcatalog*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/federated_athena_datacatalog" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaDC",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteDataCatalog",
        "athena:GetDataCatalog",
        "athena:UpdateDataCatalog"
      ],
      "Resource" : "arn:aws:athena:*:*:datacatalog/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LambdaPassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "lambda.amazonaws.com"
          ]
```

```
        }
      }
    },
    {
      "Sid" : "GetRole",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQueryExecution",
        "arn:aws:iam::*:role/datazone_s3tables_*"
      ],
      "Effect" : "Allow"
    },
    {
      "Sid" : "S3tPassConn",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:connection/aws:s3tables"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "lakeformation:EnabledOnlyForMetaDataAccess" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "GlueCatalogCreate",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCatalogMgmt",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:GetCatalogs",
        "glue:UpdateCatalog",
        "glue:DeleteCatalog",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RSManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
```

```
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:DeleteNamespace",
        "redshift-serverless:DeleteWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListSnapshotCopyConfigurations",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*",
        "arn:aws:redshift-serverless:*:*:snapshotcopyconfiguration/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataShare",
      "Effect" : "Allow",
      "Action" : [
        "redshift:AssociateDataShareConsumer",
        "redshift:AuthorizeDataShare"
      ],
      "Resource" : [
        "arn:aws:redshift:*:*:datashare:*/*"
      ],
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "redshift-serverless.amazonaws.com",
            "glue.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftBucket",
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:PutBucketPolicy",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketVersioning",
        "s3:PutBucketTagging"
      ],
      "Resource" : "arn:aws:s3:::redshift-staging-bucket-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RedshiftTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "CreateSG",
      "Effect" : "Allow",
      "Action" : [
```

```
        "ec2:CreateSecurityGroup"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "SGAuth",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SGManage",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
```

```
      "Sid" : "SGRevoke",
      "Effect" : "Allow",
      "Action" : [
        "ec2:RevokeSecurityGroupIngress"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagEc2",
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : [
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "for-use-with-amazon-emr-managed-policies",
            "aws:cloudformation:*"
          ]
        }
      }
    },
    {
      "Sid" : "EC2Describe",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNatGateways",
```

```
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeLG",
      "Effect" : "Allow",
      "Action" : "logs:DescribeLogGroups",
      "Resource" : "*"
    },
    {
      "Sid" : "CreateLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:TagResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged"
          ]
        }
      }
    },
    {
      "Sid" : "LGRetention",
      "Effect" : "Allow",
      "Action" : "logs:PutRetentionPolicy",
      "Resource" : [
```

```
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageLG",
      "Effect" : "Allow",
      "Action" : [
        "logs:DeleteLogGroup",
        "logs:UntagResource",
        "logs:DeleteRetentionPolicy",
        "logs:GetDataProtectionPolicy",
        "logs:PutDataProtectionPolicy",
        "logs:DeleteDataProtectionPolicy",
        "logs:AssociateKmsKey",
        "logs:DisassociateKmsKey",
        "logs:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:datazone-*",
        "arn:aws:logs:*:*:log-group:/aws/lambda/amazon-bedrock-ide-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AthenaManage",
      "Effect" : "Allow",
      "Action" : [
        "athena:CreateWorkGroup",
        "athena:TagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "AthenaWGDelete",
      "Effect" : "Allow",
      "Action" : [
        "athena:DeleteWorkGroup",
        "athena:UpdateWorkGroup",
        "athena:UntagResource",
        "athena:GetWorkGroup"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftCreate",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:CreateNamespace",
        "redshift-serverless:CreateWorkgroup",
        "redshift-serverless:TagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
```

```
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "TagRSS",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListTagsForResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:ResourceTag/CreatedBy" : "false"
        }
      }
    },
    {
      "Sid" : "SecretProject",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SecretAll",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "TagSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
```

```
          "aws:ResourceTag/CreatedBy" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "CreatedBy"
          ]
        }
      }
    },
    {
      "Sid" : "SecretKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
```

```
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/emr-containers.amazonaws.com/
AWSServiceRoleForAmazonEMRContainers"
      ]
    },
    {
      "Sid" : "RedshiftList",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:GetResourcePolicy"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RssDbRole",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:ExecuteStatement",
        "redshift:GetResourcePolicy",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
```

```
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift:DescribeDataSharesForConsumer",
        "redshift:DescribeDataShares"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftManage",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:UpdateNamespace",
        "redshift-serverless:UpdateWorkgroup",
        "redshift-serverless:UntagResource"
      ],
      "Resource" : [
        "arn:aws:redshift-serverless:*:*:namespace/*",
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "redshift-serverless.*.amazonaws.com"
          ]
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:redshift-serverless:arn" : "false"
        }
      }
    },
    {
      "Sid" : "GetRandom",
      "Effect" : "Allow",
      "Action" : "secretsmanager:GetRandomPassword",
      "Resource" : "*"
    },
    {
      "Sid" : "BRSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:CreateSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "RedshiftSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:RotateSecret",
        "secretsmanager:DescribeSecret",
```

```
        "secretsmanager:UpdateSecret",
        "secretsmanager:DeleteSecret"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagRsSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:TagResource"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:redshift!*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "Redshift",
            "aws:secretsmanager:*",
            "aws:redshift-serverless:*",
            "AmazonDataZone*",
            "datazone.rs.workgroup"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagSMDForUpdate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateDomain",
        "sagemaker:AddTags"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:domain/*",
        "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageSMD",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateDomain",
        "sagemaker:DeleteDomain"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:domain/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SMDManage",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListDomains",
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SMAppDelete",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteApp",
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DeleteSpace",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteSpace",
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
```

```
    },
    {
      "Sid" : "DeleteUserProfile",
      "Effect" : "Allow",
      "Action" : "sagemaker:DeleteUserProfile",
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSCreate",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:CreateApplication",
        "emr-serverless:TagResource"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "EmrSManage",
      "Effect" : "Allow",
      "Action" : [
```

```
        "emr-serverless:UpdateApplication",
        "emr-serverless:DeleteApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSGetStop",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Eni",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com",
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrSEc2Subnet",
      "Effect" : "Allow",
      "Action" : "ec2:CreateNetworkInterface",
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "ops.emr-serverless.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "MLFlowCreate",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateMlflowTrackingServer",
        "sagemaker:AddTags"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "MLFlowDescribe",
      "Effect" : "Allow",
      "Action" : "sagemaker:DescribeMlflowTrackingServer",
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*"
    },
    {
      "Sid" : "MLFlowDelete",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sagemaker:DeleteMlflowTrackingServer"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AossManage",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetAccessPolicy",
        "aoss:CreateAccessPolicy",
        "aoss:DeleteAccessPolicy",
        "aoss:UpdateAccessPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*",
          "aoss:index" : "bedrock-ide-*"
        }
      }
    },
    {
      "Sid" : "ManageAossPolicies",
      "Effect" : "Allow",
      "Action" : [
        "aoss:GetSecurityPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:DeleteSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLikeIfExists" : {
          "aoss:collection" : "bedrock-ide-*"
        }
```

```
      }
    },
    {
      "Sid" : "GetAoss",
      "Effect" : "Allow",
      "Action" : "aoss:BatchGetCollection",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AossCollections",
      "Effect" : "Allow",
      "Action" : [
        "aoss:CreateCollection",
        "aoss:UpdateCollection",
        "aoss:DeleteCollection",
        "aoss:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:CreateGraph",
        "neptune-graph:UpdateGraph",
        "neptune-graph:DeleteGraph",
        "neptune-graph:ListGraphs",
        "neptune-graph:GetGraph"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3VectorsManage",
      "Effect" : "Allow",
      "Action" : [
        "s3vectors:CreateVectorBucket",
        "s3vectors:DeleteVectorBucket",
        "s3vectors:ListVectorBuckets",
        "s3vectors:GetVectorBucket",
        "s3vectors:CreateIndex",
        "s3vectors:DeleteIndex",
        "s3vectors:ListIndexes",
        "s3vectors:GetIndex"
      ],
      "Resource" : "arn:aws:s3vectors:*:*:bucket/amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagNeptune",
      "Effect" : "Allow",
      "Action" : [
        "neptune-graph:TagResource"
      ],
      "Resource" : "arn:aws:neptune-graph:*:*:graph/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrock*"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "GetS3GenAI",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource" : "arn:aws:s3:::*/dzd*/*/genAI/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetBR",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetKnowledgeBase",
        "bedrock:GetGuardrail",
        "bedrock:GetPrompt",
        "bedrock:GetFlow",
        "bedrock:GetFlowAlias",
        "bedrock:ListTagsForResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "BRManage",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:CreateAgent",
        "bedrock:UpdateAgent",
        "bedrock:PrepareAgent",
        "bedrock:DeleteAgent",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentAlias",
        "bedrock:CreateAgentAlias",
```

```
        "bedrock:UpdateAgentAlias",
        "bedrock:DeleteAgentAlias",
        "bedrock:ListAgentActionGroups",
        "bedrock:GetAgentActionGroup",
        "bedrock:CreateAgentActionGroup",
        "bedrock:UpdateAgentActionGroup",
        "bedrock:DeleteAgentActionGroup",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:AssociateAgentKnowledgeBase",
        "bedrock:DisassociateAgentKnowledgeBase",
        "bedrock:UpdateAgentKnowledgeBase",
        "bedrock:CreateKnowledgeBase",
        "bedrock:UpdateKnowledgeBase",
        "bedrock:DeleteKnowledgeBase",
        "bedrock:ListDataSources",
        "bedrock:GetDataSource",
        "bedrock:CreateDataSource",
        "bedrock:UpdateDataSource",
        "bedrock:DeleteDataSource",
        "bedrock:ListIngestionJobs",
        "bedrock:GetIngestionJob",
        "bedrock:StartIngestionJob",
        "bedrock:StopIngestionJob",
        "bedrock:CreateGuardrail",
        "bedrock:UpdateGuardrail",
        "bedrock:DeleteGuardrail",
        "bedrock:CreateGuardrailVersion",
        "bedrock:CreatePrompt",
        "bedrock:UpdatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:CreateFlow",
        "bedrock:UpdateFlow",
        "bedrock:PrepareFlow",
        "bedrock:DeleteFlow",
        "bedrock:ListFlowAliases",
        "bedrock:GetFlowAlias",
        "bedrock:CreateFlowAlias",
        "bedrock:UpdateFlowAlias",
        "bedrock:DeleteFlowAlias",
        "bedrock:ListFlowVersions",
        "bedrock:GetFlowVersion",
        "bedrock:CreateFlowVersion",
```

```
        "bedrock:DeleteFlowVersion",
        "bedrock:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "TagBR",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : [
        "arn:aws:bedrock:*:*:agent-alias/*/TSTALIASID",
        "arn:aws:bedrock:*:*:flow/*/alias/TSTALIASID"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ListBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "ManageBRJobs",
      "Effect" : "Allow",
      "Action" : "bedrock:BatchDeleteEvaluationJob",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:CreateFunction",
        "lambda:InvokeFunction",
        "lambda:DeleteFunction",
        "lambda:UpdateFunctionCode",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration",
        "lambda:ListVersionsByFunction",
        "lambda:PublishVersion",
        "lambda:GetPolicy",
        "lambda:AddPermission",
        "lambda:TagResource"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageBRLambda",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetFunction",
        "lambda:ListTags",
        "lambda:RemovePermission"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "EMRManage",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:CreateSecurityConfiguration",
        "elasticmapreduce:DeleteSecurityConfiguration",
        "elasticmapreduce:DescribeSecurityConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterManage",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:AddJobFlowSteps",
        "elasticmapreduce:AddTags",
        "elasticmapreduce:DescribeJobFlows",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ModifyInstanceFleet",
        "elasticmapreduce:RunJobFlow",
        "elasticmapreduce:SetTerminationProtection",
        "elasticmapreduce:TerminateJobFlows",
        "elasticmapreduce:DescribeCluster"
      ],
      "Resource" : "arn:aws:elasticmapreduce:*:*:cluster/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowEnv",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:DeleteEnvironment",
        "airflow:TagResource"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AirflowGet",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "VpcCreate",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ]
    },
    {
      "Sid" : "ENICreate",
```

```
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "KmsCreate",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "airflow.*.amazonaws.com",
            "neptune-graph.*.amazonaws.com",
            "s3vectors.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "QueryRoleManage",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:CreateRole",
        "iam:DetachRolePolicy",
        "iam:DeleteRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "StringEquals" : {
          "iam:PermissionsBoundary" : "arn:aws:iam::aws:policy/
SageMakerStudioProjectUserRolePermissionsBoundary"
        }
      }
    },
    {
      "Sid" : "QueryRoleCreate",
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateRole"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "QueryRolePolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ArnEquals" : {
          "iam:PolicyARN" : [
            "arn:aws:iam::aws:policy/service-role/
SageMakerStudioQueryExecutionRolePolicy"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "TagQueryRole",
      "Effect" : "Allow",
      "Action" : "iam:TagRole",
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "CreatedForUseWithSageMakerStudio",
            "SageMakerStudioQueryExecutionRole"
          ]
        }
      }
    },
    {
      "Sid" : "ListQueryPolicy",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies"
      ],
      "Resource" : "arn:aws:iam::*:role/SageMakerStudioQueryExecutionRole"
    },
    {
      "Sid" : "EMRCleanup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteTags"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrRoleCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:DeleteRolePolicy",
```

```
        "iam:DeleteRole"
      ],
      "Resource" : "arn:aws:iam::*:role/datazone_emr_*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EmrInstanceCleanup",
      "Effect" : "Allow",
      "Action" : [
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile"
      ],
      "Resource" : "arn:aws:iam::*:instance-profile/
datazone_emr_ec2_instance_profile_*"
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:ListTagsForResource",
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ScheduleGroup",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteScheduleGroup",
        "scheduler:UntagResource"
      ],
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "CreateSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:CreateScheduleGroup",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:RequestTag/AmazonDataZoneProject" : "false",
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "TagSchedule",
      "Effect" : "Allow",
      "Action" : "scheduler:TagResource",
      "Resource" : "arn:aws:scheduler:*:*:schedule-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:TagKeys" : "false",
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : "AmazonDataZone*"
        }
      }
    },
    {
      "Sid" : "DeleteSchedule",
```

```
      "Effect" : "Allow",
      "Action" : [
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/SageMakerUnifiedStudio-*-*/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageQSFolder",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSource",
        "quicksight:CreateFolder",
        "quicksight:CreateFolderMembership",
        "quicksight:CreateVPCConnection",
        "quicksight:DeleteDataSource",
        "quicksight:DeleteFolder",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolderPermissions",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:DeleteVPCConnection",
        "quicksight:ListFolderMembers",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDataSource",
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:UpdateFolder",
        "quicksight:UpdateFolderPermissions",
        "quicksight:UpdateVPCConnection"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "QuickSightResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeDataSet",
        "quicksight:DescribeDashboard",
        "quicksight:DescribeDashboardPermissions",
        "quicksight:DescribeFolder",
        "quicksight:DescribeGroup",
        "quicksight:DescribeGroupMembership",
        "quicksight:DescribeUser",
        "quicksight:DescribeVPCConnection",
        "quicksight:ListTagsForResource",
        "quicksight:UpdateDashboardPermissions"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagQS",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:TagResource"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ],
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
```

```
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "PassRoleForQS",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMakerQuickSightVPC",
        "arn:aws:iam::*:role/datazone_usr_role_*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "quicksight.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "PutRule",
      "Effect" : "Allow",
      "Action" : "events:PutRule",
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "events:source" : [
            "aws.quicksight",
            "aws.codecommit"
          ]
        },
        "Null" : {
          "events:source" : "false",
          "events:detail-type" : "false"
        },
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "events:detail-type" : [
            "AWS Service Event via CloudTrail",
            "CodeCommit Repository State Change"
```

```
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:DeleteRule",
        "events:DisableRule",
        "events:EnableRule",
        "events:PutTargets",
        "events:RemoveTargets"
      ],
      "Resource" : "arn:aws:events:*:*:rule/Managed.SageMaker*",
      "Condition" : {
        "StringEquals" : {
          "events:ManagedBy" : "datazone.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "RssAdmin",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3AGPerm",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstance",
```

```
        "s3:CreateAccessGrantsInstance"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ResourceTagsUnTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:UntagResource",
        "neptune-graph:UntagResource",
        "quicksight:UntagResource",
        "glue:UntagResource",
        "airflow:UntagResource",
        "secretsmanager:UntagResource",
        "lambda:UntagResource",
        "emr-serverless:UntagResource",
        "elasticmapreduce:RemoveTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "SSOManage",
      "Effect" : "Allow",
      "Action" : [
        "sso:CreateApplication",
        "sso:DeleteApplication",
        "sso:DescribeApplication",
        "sso:DescribeInstance",
        "sso:ListInstances",
        "sso:PutApplicationAccessScope",
```

```
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant",
        "sso:PutApplicationSessionConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "elasticmapreduce.amazonaws.com",
            "emr-containers.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "ops.emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EksClusterDiscovery",
      "Effect" : "Allow",
      "Action" : [
        "eks:DescribeCluster"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EmrContainersManage",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:CreateManagedEndpoint",
        "emr-containers:CreateSecurityConfiguration",
        "emr-containers:CreateVirtualCluster",
        "emr-containers:DeleteManagedEndpoint",
        "emr-containers:DeleteSecurityConfiguration",
        "emr-containers:DeleteVirtualCluster",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "ManageViaEmrContainers",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeNetworkInterfaces",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "eks:AssociateAccessPolicy",
        "eks:CreateAccessEntry",
        "eks:DisassociateAccessPolicy",
        "eks:DeleteAccessEntry",
        "eks:DescribeAccessEntry",
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioProjectRoleMachineLearningPolicy

Beschreibung: Amazon SageMaker Studio erstellt IAM-Rollen für Projektbenutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die zugehörigen Berechtigungen zu SageMaker definieren.

`SageMakerStudioProjectRoleMachineLearningPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioProjectRoleMachineLearningPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2024, 21:55 UTC
- Bearbeitete Zeit: 21. November 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectRoleMachineLearningPolicy`

Version der Richtlinie

Richtlinienversion: v12 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowManageSageMakerEniOnVpc",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : [
            "sagemaker.amazonaws.com",
            "airflow.amazonaws.com"
          ]
        },
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
      "Sid" : "AllowManageSageMakerTrainingEniOnVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
      "Condition" : {
        "ArnLike" : {
          "ec2:Vpc" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}"
        }
      }
    },
    {
```

```
      "Sid" : "AllowManageSageMakerEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition" : {
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpointOnVpcId",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : "arn:aws:ec2:*:*:vpc/${aws:PrincipalTag/VpcId}",
      "Condition" : {
        "StringEquals" : {
          "ec2:VpcID" : "${aws:PrincipalTag/VpcId}"
        },
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerCreateVpcEndpoint",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateVpcEndpoint"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:vpc-endpoint/*"
      ],
      "Condition" : {
```

```
        "StringEqualsIfExists" : {
          "aws:CalledViaLast" : "sagemaker.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowSageMakerDescribeVPCResources",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "glue:ListSessions",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowSageMakerLogAccess",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:GetLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerMlflowPermission",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:mlflow-tracking-server/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerBYOFSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticfilesystem:DescribeMountTargets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerBYOIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImageVersion",
        "sagemaker:ListImageVersions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeImageActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeImage"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:image/*"
    },
    {
      "Sid" : "SageMakerPipelinesSTSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sts:GetCallerIdentity"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    {
      "Sid" : "SageMakerCreatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateInferenceRecommendationsJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerInferencePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
```

```
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUpdateInferenceComponentRuntimeConfigAutoscalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:UpdateInferenceComponentRuntimeConfig"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerDescribeUpdateDeletePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:UpdatePipeline",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DeletePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopPipelineExecution",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:AddAssociation",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
```

```
        "sagemaker:DeleteArtifact"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerModelRegistryLineageSpecialPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:QueryLineage",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:GetSearchSuggestions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelines",
```

```
        "sagemaker:ListContexts"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerSearchPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Search"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true",
          "sagemaker:SearchVisibilityCondition/Tags.AmazonDataZoneProject/
EqualsIfExists" : "${aws:PrincipalTag/AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerListPermissionsTagRestricted",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
```

```
    },
    {
      "Sid" : "SageMakerECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*"
    },
    {
      "Sid" : "SageMakerECRGetAuthorizationTokenPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:GetAuthorizationToken"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupGetPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupListPermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:ListGroupResources"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupWritePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "AmazonSageMakerModelRegistryResourceGroupDeletePermission",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerMLFlowModelRegistrationPermission",
```

```
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackageGroup"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:model-package-group/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioCreatePresignedDomainUrlForTaggedUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "aws:PrincipalTag/EnableSageMakerMLWorkloadsPermissions" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "SageMakerStudioAppListActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerStudioAppDescribeDomainActionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeDomain"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeJupyterLabAppActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ]
    },
    {
      "Sid" : "SageMakerStudioAppDescribeUserProfileActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAppDescribeTaggedUserProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SMStudioAppDescribeSpaceActionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeSpace"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        },
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*/${aws:PrincipalTag/
datazone:userId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioAllowCreatingDeletingTaggedOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateSpace",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
```

```
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUserProfile",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        },
        "ArnLike" : {
          "sagemaker:OwnerUserProfileArn" : "arn:aws:sagemaker:*:*:user-profile/*/
${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerStudioRestrictPrivateSpaceAppsToOwnerUser",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:DeleteApp"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:app/*/*/CodeEditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/codeeditor/*",
        "arn:aws:sagemaker:*:*:app/*/*/jupyterlab/*",
        "arn:aws:sagemaker:*:*:app/*/*/JupyterLab/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "PublishSagemakerMetric",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "/aws/sagemaker/*"
        }
      }
    },
    {
      "Sid" : "ManageSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudwatch:DescribeAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "MutateSageMakerEndpointsAutoscalingAlarms",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "arn:aws:cloudwatch:*:*:alarm:TargetTracking*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:CalledViaLast" : "application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SSMPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource" : "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
    },
    {
      "Sid" : "SageMakerJumpstartS3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::jumpstart-cache-prod-*/*"
      ],
      "Condition" : {
```

```
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerCrossAccountPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:ListModelPackages",
        "sagemaker:CreateModel"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerListTagsRestrictionOnSharedResources",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListTags"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissionsWithserviceNamespace",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:PutScalingPolicy",
```

```
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "application-autoscaling:service-namespace" : "sagemaker"
        }
      }
    },
    {
      "Sid" : "SageMakerAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions"
      ],
      "Resource" : "arn:aws:application-autoscaling:*:*:scalable-target/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SageMakerKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
```

```
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGObjectRead",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGObjectWrite",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
```

```
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGBucketLevelReadPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnEquals" : {
          "s3:AccessGrantsInstanceArn" : [
            "arn:aws:s3:*:*:access-grants/default"
          ]
        }
      }
    },
    {
      "Sid" : "S3AGKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
```

```
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "S3AGLocationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrantsLocation",
        "s3:DeleteAccessGrantsLocation",
        "s3:GetAccessGrantsLocation"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "s3:accessGrantsLocationScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/"
        }
      }
    },
    {
      "Sid" : "S3AGPermissionManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateAccessGrant",
        "s3:DeleteAccessGrant"
      ],
      "Resource" : [
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringLike" : {
```

```
          "s3:accessGrantScope" : "s3://${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "s3:AccessGrants"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3AGResourceSharingPolicyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:PutAccessGrantsInstanceResourcePolicy"
      ],
      "Resource" : "arn:aws:s3:*:*:access-grants/default",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3AGTaggingPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:TagResource",
        "s3:ListTagsForResource"
      ],
      "Resource" : [
```

```
        "arn:aws:s3:*:*:access-grants/default/location/*",
        "arn:aws:s3:*:*:access-grants/default/grant/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ConsumerS3AGPermission",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetAccessGrantsInstanceForPrefix",
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "ram:GetResourceShareInvitations"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioProjectUserRolePermissionsBoundary

Beschreibung: Amazon SageMaker erstellt IAM-Rollen für Projects-Benutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Grenze ihrer Berechtigungen zu definieren.

`SageMakerStudioProjectUserRolePermissionsBoundary`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioProjectUserRolePermissionsBoundary` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2024, 21:57 UTC
- Zeit bearbeitet: 03. Januar 2025, 00:37 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePermissionsBoundary`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DenyAllNonMatchingProjectTag",
      "Effect" : "Deny",
      "Action" : "*",
      "NotResource" : [
        "arn:*:sagemaker:*:*:model-package-group/*",
        "arn:*:sagemaker:*:*:model-package/*",
        "arn:*:glue:*:*:catalog/*",
        "arn:*:glue:*:*:database/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false",
```

```
          "aws:PrincipalTag/AmazonDataZoneProject" : "false",
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        },
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "redshift-serverless.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "ec2.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AllowGenerateDataKeyForEmrEbsEncryption",
      "Effect" : "Allow",
      "Action" : "kms:GenerateDataKey",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SameAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com",
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket",
```

```
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "CrossAccountKMSManagementPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListGrants",
        "kms:GetPublicKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
        "*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "DataZoneDescribeKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
```

```
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
 "arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessCertificateS3LocationPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/certificate_location/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : ""
        },
        "Null" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : "false"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
```

```
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "CloudWatchDescribeLogGroups",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CloudWatchLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:StartQuery",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:airflow*",
        "arn:aws:logs:*:*:log-group:datazone*"
      ]
    },
    {
```

```
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
```

```
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataZonePermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
```

```
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
```

```
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
```

```
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:UseGlueStudio",
        "glue:ListSessions",
        "glue:StartCompletion",
        "glue:GetCompletion",
        "glue:GetGeneratedCode",
        "glue:GetTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GluePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:CancelStatement",
        "glue:ListStatements",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
```

```
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
```

```
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "IAMPassRolePermission",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
```

```
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "ec2.amazonaws.com",
            "emr-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftUnrestrictedPermissions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:GetQCustomContext",
```

```
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQSqlPromptQuotas",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftPermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
```

```
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : "redshift-data.amazonaws.com"
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
```

```
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "GenerativeAIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockAppInferenceProfileInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockModelInvocationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*:*:*-model/*"
      ],
      "Condition" : {
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
```

```
      }
    },
    {
      "Sid" : "ManageNetworkPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DeleteNetworkInterface",
        "ec2:DetachNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:ListImageVersions",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListEndpoints",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListModels",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModelPackageGroups",
```

```
        "sagemaker:ListModelMetadata",
        "sagemaker:ListMlflowTrackingServers",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListApps",
        "sagemaker:ListDomains",
        "sagemaker:ListUserProfiles",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeUserProfile",
        "sagemaker:DescribeSpace",
        "sagemaker:AddTags",
        "sagemaker:AddAssociation",
```

```
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteUserProfile",
        "sagemaker:UpdateSpace",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteApp",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:CreateSpace",
        "sagemaker:CreateApp",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePipeline",
        "sagemaker:CreateContext",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAction",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateTrainingJob",
        "sagemaker:BatchGetMetrics",
        "sagemaker:BatchPutMetrics",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteEndpoint",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:UpdateModelPackage",
```

```
            "sagemaker:DeleteModel",
            "sagemaker:DeleteModelPackage",
            "sagemaker:DeleteModelPackageGroup",
            "sagemaker:DeleteTags",
            "sagemaker:DeleteInferenceComponent",
            "sagemaker:CreateInferenceRecommendationsJob",
            "sagemaker:InvokeEndpoint",
            "sagemaker:InvokeEndpointAsync",
            "sagemaker:InvokeEndpointWithResponseStream",
            "sagemaker:QueryLineage",
            "sagemaker:UpdatePipeline",
            "sagemaker:DeletePipeline",
            "sagemaker:UpdatePipelineExecution",
            "sagemaker:StartPipelineExecution",
            "sagemaker:StopPipelineExecution",
            "sagemaker:RetryPipelineExecution",
            "sagemaker:SendPipelineExecutionStepSuccess",
            "sagemaker:SendPipelineExecutionStepFailure",
            "sagemaker:GetSearchSuggestions",
            "sagemaker:Search",
            "sagemaker:UpdateMlflowTrackingServer",
            "sagemaker:StartMlflowTrackingServer",
            "sagemaker:StopMlflowTrackingServer",
            "sagemaker:CreatePresignedMlflowTrackingServerUrl",
            "sagemaker:ListPartnerApps",
            "sagemaker:CreatePartnerAppPresignedUrl",
            "sagemaker:DescribePartnerApp",
            "sagemaker:CallPartnerAppApi",
            "sagemaker-mlflow:AccessUI",
            "sagemaker-mlflow:CreateExperiment",
            "sagemaker-mlflow:SearchExperiments",
            "sagemaker-mlflow:GetExperiment",
            "sagemaker-mlflow:GetExperimentByName",
            "sagemaker-mlflow:DeleteExperiment",
            "sagemaker-mlflow:RestoreExperiment",
            "sagemaker-mlflow:UpdateExperiment",
            "sagemaker-mlflow:CreateRun",
            "sagemaker-mlflow:DeleteRun",
            "sagemaker-mlflow:RestoreRun",
            "sagemaker-mlflow:GetRun",
            "sagemaker-mlflow:LogMetric",
            "sagemaker-mlflow:LogBatch",
            "sagemaker-mlflow:LogModel",
            "sagemaker-mlflow:LogInputs",
```

```
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker-mlflow:CreateRegisteredModel",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "ecr:GetAuthorizationToken",
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer",
        "ecr:DescribeImages",
        "elasticfilesystem:DescribeMountTargets",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerSLRForAutoScalingPermissions",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
```

```
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sagemaker.application-autoscaling.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "ComputePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:GetMetricData",
        "sts:GetCallerIdentity",
        "sts:TagSession",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
        "sts:AssumeRole"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputePermissionsWithResourceTag",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables",
        "elasticmapreduce:GetClusterSessionCredentials",
```

```
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:TerminateJobFlows",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "DataLakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
```

```
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
```

```
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "EMRServicePermissions",
      "Effect" : "Allow",
      "Action" : [
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:RegisterScalableTarget",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScheduledAction",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "ec2:RunInstances",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeletePlacementGroup",
        "ec2:ModifyInstanceAttribute",
        "ec2:TerminateInstances",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
```

```
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupGetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ModelRegistryResourceGroupMutatePermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/sagemaker:collection" : "false"
        }
      }
    },
    {
      "Sid" : "ModelRegistryBedRockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AccessAossCollectionsForBedrock",
      "Effect" : "Allow",
      "Action" : "aoss:APIAccessAll",
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "AccessBedrockResources",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetAgent",
        "bedrock:GetAgentActionGroup",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:InvokeAgent",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ListIngestionJobs",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "CreateEvaluationJobForFoundationModel",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*"
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*"
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockKnowledgeBaseDataIngestionKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/AmazonBedrockManaged" : "true"
        },
        "Null" : {
          "kms:ViaService" : "true",
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForBedrockApp",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetDataZoneEnvironmentCfnStackPermissionsForBedrockAppExport",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "MWAAPermissions",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments",
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment",
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
```

```
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
    },
    {
      "Sid" : "SQSPermissionsForMWAA",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : "arn:aws:sqs:*:*:airflow-celery-*"
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
```

```
      }
    },
    {
      "Sid" : "GlueConnectionAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SecretAccessForForUseWithAllDataZoneProjectsSecrets",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "AccessForDynamoDbConnections",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
```

```
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketForQueryExecutionRolePermissions",
      "Effect" : "Allow",
      "Action" : "s3:ListBucket",
      "Resource" : "arn:aws:s3:::*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "S3PermissionsForAthenaCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource" : [
        "arn:aws:s3:::redshift-staging-bucket-*/*",
        "arn:aws:s3:::redshift-staging-bucket-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetS3ObjectForQueryExecutionRolePermissions",
      "Effect" : "Allow",
```

```
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::*/dzd_*/*/dev/sys/athena/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
```

```
    {
      "Sid" : "NotDeniedOperations",
      "Effect" : "Deny",
      "NotAction" : [
        "airflow:CreateWebLoginToken",
        "airflow:GetEnvironment",
        "airflow:InvokeRestApi",
        "airflow:ListEnvironments",
        "airflow:UpdateEnvironment",
        "aoss:APIAccessAll",
        "application-autoscaling:DeleteScalingPolicy",
        "application-autoscaling:DeleteScheduledAction",
        "application-autoscaling:DeregisterScalableTarget",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingActivities",
        "application-autoscaling:DescribeScalingPolicies",
        "application-autoscaling:DescribeScheduledActions",
        "application-autoscaling:PutScalingPolicy",
        "application-autoscaling:PutScheduledAction",
        "application-autoscaling:RegisterScalableTarget",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
```

```
            "athena:GetSessionStatus",
            "athena:GetTableMetadata",
            "athena:GetWorkGroup",
            "athena:ImportNotebook",
            "athena:ListDatabases",
            "athena:ListDataCatalogs",
            "athena:ListEngineVersions",
            "athena:ListNamedQueries",
            "athena:ListPreparedStatements",
            "athena:ListQueryExecutions",
            "athena:ListTableMetadata",
            "athena:ListTagsForResource",
            "athena:ListWorkGroups",
            "athena:StartCalculationExecution",
            "athena:StartQueryExecution",
            "athena:StartSession",
            "athena:StopCalculationExecution",
            "athena:StopQueryExecution",
            "athena:TerminateSession",
            "athena:UpdateNamedQuery",
            "athena:UpdateNotebook",
            "athena:UpdateNotebookMetadata",
            "athena:UpdatePreparedStatement",
            "bedrock:ApplyGuardrail",
            "bedrock:BatchDeleteEvaluationJob",
            "bedrock:CreateAgentAlias",
            "bedrock:CreateEvaluationJob",
            "bedrock:CreatePrompt",
            "bedrock:CreatePromptVersion",
            "bedrock:DeleteAgentAlias",
            "bedrock:DeleteAgentVersion",
            "bedrock:DeletePrompt",
            "bedrock:GetAgent",
            "bedrock:GetAgentActionGroup",
            "bedrock:GetAgentAlias",
            "bedrock:GetAgentKnowledgeBase",
            "bedrock:GetAgentVersion",
            "bedrock:GetEvaluationJob",
            "bedrock:GetInferenceProfile",
            "bedrock:GetIngestionJob",
            "bedrock:GetPrompt",
            "bedrock:InvokeAgent",
            "bedrock:InvokeFlow",
            "bedrock:InvokeInlineAgent",
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgentVersions",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFoundationModels",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:RetrieveAndGenerate",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
        "bedrock:TagResource",
        "bedrock:UpdateAgentAlias",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate",
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:PutMetricData",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:BatchGetCommits",
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
```

```
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codewhisperer:GenerateRecommendations",
        "datazone:CreateConnection",
```

```
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironments",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "dynamodb:BatchGetItem",
        "dynamodb:BatchWriteItem",
        "dynamodb:Scan",
        "dynamodb:Query",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContributorInsights",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeEndpoints",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeImport",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTableReplicaAutoScaling",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:GetItem",
        "dynamodb:GetRecords",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListImports",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "dynamodb:PutItem",
        "dynamodb:PartiQLSelect",
        "dynamodb:PartiQLInsert",
        "dynamodb:PartiQLUpdate",
```

```
        "dynamodb:PartiQLDelete",
        "dynamodb:UpdateItem",
        "dynamodb:UpdateGlobalTable",
        "dynamodb:UpdateTable",
        "ec2:AttachNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateFleet",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:CreatePlacementGroup",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteTags",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeCapacityReservations",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcs",
        "ec2:DetachNetworkInterface",
        "ec2:ModifyInstanceAttribute",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "elasticfilesystem:DescribeMountTargets",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:DescribePersistentAppUI",
        "elasticmapreduce:GetClusterSessionCredentials",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL",
        "elasticmapreduce:GetPersistentAppUIPresignedURL",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:TerminateJobFlows",
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRunAttempts",
        "emr-serverless:ListJobRuns",
        "emr-serverless:StartApplication",
        "emr-serverless:StartJobRun",
        "emr-serverless:StopApplication",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:CancelStatement",
```

```
        "glue:CreateBlueprint",
        "glue:CreateDatabase",
        "glue:CreateDataQualityRuleset",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateSession",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteDatabase",
        "glue:DeleteDataQualityRuleset",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteSession",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:DescribeConnectionType",
        "glue:DescribeEntity",
        "glue:GetCatalog",
        "glue:GetCatalogImportStatus",
        "glue:GetCatalogs",
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetCompletion",
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetDashboardUrl",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
```

```
            "glue:GetEntityRecords",
            "glue:GetGeneratedCode",
            "glue:GetPartition",
            "glue:GetPartitionIndexes",
            "glue:GetPartitions",
            "glue:GetSession",
            "glue:GetStatement",
            "glue:GetTable",
            "glue:GetTableOptimizer",
            "glue:GetTables",
            "glue:GetTableVersion",
            "glue:GetTableVersions",
            "glue:GetTags",
            "glue:GetUserDefinedFunction",
            "glue:GetUserDefinedFunctions",
            "glue:ListConnectionTypes",
            "glue:ListCrawls",
            "glue:ListDataQualityResults",
            "glue:ListDataQualityRuleRecommendationRuns",
            "glue:ListDataQualityRulesetEvaluationRuns",
            "glue:ListDataQualityRulesets",
            "glue:ListEntities",
            "glue:ListSessions",
            "glue:ListStatements",
            "glue:ListTableOptimizerRuns",
            "glue:NotifyEvent",
            "glue:PassConnection",
            "glue:PublishDataQuality",
            "glue:PutDataQualityProfileAnnotation",
            "glue:PutDataQualityStatisticAnnotation",
            "glue:PutWorkflowRunProperties",
            "glue:ResumeWorkflowRun",
            "glue:RunStatement",
            "glue:SearchTables",
            "glue:StartBlueprintRun",
            "glue:StartCompletion",
            "glue:StartDataQualityRuleRecommendationRun",
            "glue:StartDataQualityRulesetEvaluationRun",
            "glue:StartJobRun",
            "glue:StartWorkflowRun",
            "glue:StopSession",
            "glue:StopWorkflowRun",
            "glue:TagResource",
            "glue:UntagResource",
```

```
        "glue:UpdateBlueprint",
        "glue:UpdateCatalog",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDataQualityRuleset",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "glue:UseGlueStudio",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:GetPublicKey",
        "kms:ListAliases",
        "kms:ListGrants",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "lakeformation:GetDataAccess",
        "lambda:InvokeFunction",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetLogRecord",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:StartQuery",
        "logs:StopQuery",
        "pricing:GetProducts",
        "q:SendMessage",
        "q:StartConversation",
        "redshift-data:BatchExecuteStatement",
```

```
        "redshift-data:CancelStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-data:GetStatementResult",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListStatements",
        "redshift-data:ListTables",
        "redshift-serverless:GetCredentials",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters",
        "redshift:DescribeTags",
        "redshift:GetClusterCredentialsWithIAM",
        "resource-groups:CreateGroup",
        "resource-groups:DeleteGroup",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources",
        "resource-groups:Tag",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketLocation",
        "s3:GetEncryptionConfiguration",
        "s3:GetObject*",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:PutObjectTagging",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "sagemaker-mlflow:AccessUI",
        "sagemaker-mlflow:CreateExperiment",
        "sagemaker-mlflow:CreateModelVersion",
        "sagemaker-mlflow:CreateRegisteredModel",
```

```
        "sagemaker-mlflow:CreateRun",
        "sagemaker-mlflow:DeleteExperiment",
        "sagemaker-mlflow:DeleteModelVersion",
        "sagemaker-mlflow:DeleteModelVersionTag",
        "sagemaker-mlflow:DeleteRegisteredModel",
        "sagemaker-mlflow:DeleteRegisteredModelAlias",
        "sagemaker-mlflow:DeleteRegisteredModelTag",
        "sagemaker-mlflow:DeleteRun",
        "sagemaker-mlflow:DeleteTag",
        "sagemaker-mlflow:GetDownloadURIForModelVersionArtifacts",
        "sagemaker-mlflow:GetExperiment",
        "sagemaker-mlflow:GetExperimentByName",
        "sagemaker-mlflow:GetLatestModelVersions",
        "sagemaker-mlflow:GetMetricHistory",
        "sagemaker-mlflow:GetModelVersion",
        "sagemaker-mlflow:GetModelVersionByAlias",
        "sagemaker-mlflow:GetRegisteredModel",
        "sagemaker-mlflow:GetRun",
        "sagemaker-mlflow:ListArtifacts",
        "sagemaker-mlflow:LogBatch",
        "sagemaker-mlflow:LogInputs",
        "sagemaker-mlflow:LogMetric",
        "sagemaker-mlflow:LogModel",
        "sagemaker-mlflow:LogParam",
        "sagemaker-mlflow:RenameRegisteredModel",
        "sagemaker-mlflow:RestoreExperiment",
        "sagemaker-mlflow:RestoreRun",
        "sagemaker-mlflow:SearchExperiments",
        "sagemaker-mlflow:SearchModelVersions",
        "sagemaker-mlflow:SearchRegisteredModels",
        "sagemaker-mlflow:SearchRuns",
        "sagemaker-mlflow:SetExperimentTag",
        "sagemaker-mlflow:SetRegisteredModelAlias",
        "sagemaker-mlflow:SetRegisteredModelTag",
        "sagemaker-mlflow:SetTag",
        "sagemaker-mlflow:TransitionModelVersionStage",
        "sagemaker-mlflow:UpdateExperiment",
        "sagemaker-mlflow:UpdateModelVersion",
        "sagemaker-mlflow:UpdateRegisteredModel",
        "sagemaker-mlflow:UpdateRun",
        "sagemaker:AddAssociation",
        "sagemaker:AddTags",
        "sagemaker:BatchDescribeModelPackage",
        "sagemaker:BatchGetMetrics",
```

```
        "sagemaker:BatchPutMetrics",
        "sagemaker:CallPartnerAppApi",
        "sagemaker:CreateAction",
        "sagemaker:CreateApp",
        "sagemaker:CreateArtifact",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateAutoMLJobV2",
        "sagemaker:CreateContext",
        "sagemaker:CreateEndpoint",
        "sagemaker:CreateEndpointConfig",
        "sagemaker:CreateHyperParameterTuningJob",
        "sagemaker:CreateInferenceComponent",
        "sagemaker:CreateInferenceRecommendationsJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateModelPackage",
        "sagemaker:CreateModelPackageGroup",
        "sagemaker:CreatePartnerAppPresignedUrl",
        "sagemaker:CreatePipeline",
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker:CreateProcessingJob",
        "sagemaker:CreateSpace",
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateTransformJob",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteAction",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteArtifact",
        "sagemaker:DeleteAssociation",
        "sagemaker:DeleteContext",
        "sagemaker:DeleteEndpoint",
        "sagemaker:DeleteEndpointConfig",
        "sagemaker:DeleteInferenceComponent",
        "sagemaker:DeleteModel",
        "sagemaker:DeleteModelPackage",
        "sagemaker:DeleteModelPackageGroup",
        "sagemaker:DeletePipeline",
        "sagemaker:DeleteSpace",
        "sagemaker:DeleteTags",
        "sagemaker:DeleteUserProfile",
        "sagemaker:DescribeAction",
        "sagemaker:DescribeApp",
        "sagemaker:DescribeArtifact",
        "sagemaker:DescribeAutoMLJob",
```

```
        "sagemaker:DescribeAutoMLJobV2",
        "sagemaker:DescribeContext",
        "sagemaker:DescribeDomain",
        "sagemaker:DescribeEndpoint",
        "sagemaker:DescribeEndpointConfig",
        "sagemaker:DescribeHyperParameterTuningJob",
        "sagemaker:DescribeImage",
        "sagemaker:DescribeImageVersion",
        "sagemaker:DescribeInferenceComponent",
        "sagemaker:DescribeInferenceRecommendationsJob",
        "sagemaker:DescribeMlflowTrackingServer",
        "sagemaker:DescribeModel",
        "sagemaker:DescribeModelPackage",
        "sagemaker:DescribeModelPackageGroup",
        "sagemaker:DescribeOptimizationJob",
        "sagemaker:DescribePartnerApp",
        "sagemaker:DescribePipeline",
        "sagemaker:DescribePipelineDefinitionForExecution",
        "sagemaker:DescribePipelineExecution",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeSpace",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:DescribeTrialComponent",
        "sagemaker:DescribeUserProfile",
        "sagemaker:GetSearchSuggestions",
        "sagemaker:InvokeEndpoint",
        "sagemaker:InvokeEndpointAsync",
        "sagemaker:InvokeEndpointWithResponseStream",
        "sagemaker:ListApps",
        "sagemaker:ListArtifacts",
        "sagemaker:ListAssociations",
        "sagemaker:ListAutoMLJobs",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:ListContexts",
        "sagemaker:ListDomains",
        "sagemaker:ListEndpointConfigs",
        "sagemaker:ListEndpoints",
        "sagemaker:ListHubContents",
        "sagemaker:ListHubs",
        "sagemaker:ListHyperParameterTuningJobs",
        "sagemaker:ListImageVersions",
        "sagemaker:ListInferenceComponents",
        "sagemaker:ListMlflowTrackingServers",
```

```
        "sagemaker:ListModelMetadata",
        "sagemaker:ListModelPackageGroups",
        "sagemaker:ListModelPackages",
        "sagemaker:ListModels",
        "sagemaker:ListPartnerApps",
        "sagemaker:ListPipelineExecutions",
        "sagemaker:ListPipelineExecutionSteps",
        "sagemaker:ListPipelineParametersForExecution",
        "sagemaker:ListPipelines",
        "sagemaker:ListProcessingJobs",
        "sagemaker:ListSpaces",
        "sagemaker:ListTags",
        "sagemaker:ListTrainingJobs",
        "sagemaker:ListTrainingJobsForHyperParameterTuningJob",
        "sagemaker:ListTransformJobs",
        "sagemaker:ListUserProfiles",
        "sagemaker:QueryLineage",
        "sagemaker:RetryPipelineExecution",
        "sagemaker:Search",
        "sagemaker:SendPipelineExecutionStepFailure",
        "sagemaker:SendPipelineExecutionStepSuccess",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StartPipelineExecution",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopHyperParameterTuningJob",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:StopPipelineExecution",
        "sagemaker:StopProcessingJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:StopTransformJob",
        "sagemaker:UpdateEndpoint",
        "sagemaker:UpdateEndpointWeightsAndCapacities",
        "sagemaker:UpdateInferenceComponentRuntimeConfig",
        "sagemaker:UpdateMlflowTrackingServer",
        "sagemaker:UpdateModelPackage",
        "sagemaker:UpdatePipeline",
        "sagemaker:UpdatePipelineExecution",
        "sagemaker:UpdateSpace",
        "sagemaker:UpdateTrainingJob",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:ListSecrets",
        "secretsmanager:PutSecretValue",
        "sqlworkbench:CreateConnection",
```

```
        "sqlworkbench:DeleteQCustomContext",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetAutocompletionMetadata",
        "sqlworkbench:GetAutocompletionResource",
        "sqlworkbench:GetQCustomContext",
        "sqlworkbench:GetQSqlPromptQuotas",
        "sqlworkbench:GetQSqlRecommendations",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:ListTabs",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:PutQCustomContext",
        "sqlworkbench:PutTab",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:GetParametersByPath",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "sts:SetSourceIdentity",
        "sts:TagSession",
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioProjectUserRolePolicy

Beschreibung: Amazon SageMaker Studio erstellt IAM-Rollen für Projektbenutzer, um Datenanalysen, künstliche Intelligenz und maschinelles Lernen durchzuführen, und verwendet diese Richtlinie bei der Erstellung dieser Rollen, um die Berechtigungen zu definieren.

`SageMakerStudioProjectUserRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioProjectUserRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 20. November 2024, 21:59 UTC
- Bearbeitete Zeit: 20. November 2025, 14:49 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioProjectUserRolePolicy`

Version der Richtlinie

Richtlinienversion: v21 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "CommonUserCodeCommitPermissions",
      "Effect" : "Allow",
      "Action" : [
        "codecommit:BatchGetCommits",
```

```
        "codecommit:BatchGetPullRequests",
        "codecommit:BatchGetRepositories",
        "codecommit:BatchDescribeMergeConflicts",
        "codecommit:CreateBranch",
        "codecommit:CreateCommit",
        "codecommit:CreatePullRequest",
        "codecommit:DeleteBranch",
        "codecommit:DeleteFile",
        "codecommit:DescribeMergeConflicts",
        "codecommit:DescribePullRequestEvents",
        "codecommit:GetBlob",
        "codecommit:GetBranch",
        "codecommit:GetComment",
        "codecommit:GetCommentReactions",
        "codecommit:GetCommentsForComparedCommit",
        "codecommit:GetCommentsForPullRequest",
        "codecommit:GetCommit",
        "codecommit:GetCommitHistory",
        "codecommit:GetCommitsFromMergeBase",
        "codecommit:GetDifferences",
        "codecommit:GetFile",
        "codecommit:GetFolder",
        "codecommit:GetMergeCommit",
        "codecommit:GetMergeConflicts",
        "codecommit:GetMergeOptions",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetPullRequest",
        "codecommit:GetPullRequestApprovalStates",
        "codecommit:GetPullRequestOverrideState",
        "codecommit:GetReferences",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:GetTree",
        "codecommit:GetUploadArchiveStatus",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:ListAssociatedApprovalRuleTemplatesForRepository",
        "codecommit:ListBranches",
        "codecommit:ListFileCommitHistory",
        "codecommit:ListPullRequests",
        "codecommit:ListTagsForResource",
        "codecommit:MergeBranchesByFastForward",
        "codecommit:MergeBranchesBySquash",
        "codecommit:MergeBranchesByThreeWay",
```

```
        "codecommit:MergePullRequestByFastForward",
        "codecommit:MergePullRequestBySquash",
        "codecommit:MergePullRequestByThreeWay",
        "codecommit:UpdateComment",
        "codecommit:UpdateDefaultBranch",
        "codecommit:UpdatePullRequestApprovalRuleContent",
        "codecommit:UpdatePullRequestApprovalState",
        "codecommit:UpdatePullRequestDescription",
        "codecommit:UpdatePullRequestStatus",
        "codecommit:UpdatePullRequestTitle",
        "codecommit:UpdateRepositoryDescription",
        "codecommit:PostCommentForComparedCommit",
        "codecommit:PostCommentForPullRequest",
        "codecommit:PostCommentReply",
        "codecommit:PutCommentReaction",
        "codecommit:PutFile"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CodeCommitKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "codecommit.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
```

```
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContext:aws:codecommit:id" : "false"
        }
      }
    },
    {
      "Sid" : "AllowCodeWhispererGenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowGlueCreateEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        },
        "Null" : {
          "aws:TagKeys" : "true"
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSecurityGroup",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:security-group/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
```

```
        }
      }
    },
    {
      "Sid" : "AllowGlueCreateEniOnSubnet",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:subnet/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowManageGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteNetworkInterface",
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:network-interface/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "aws:ResourceTag/aws-glue-service-resource" : "false"
        }
      }
    },
    {
      "Sid" : "AllowAttachGlueEniOnInstance",
      "Effect" : "Allow",
      "Action" : [
        "ec2:AttachNetworkInterface"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
```

```
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDescribeGlueEni",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionGlueSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueKernelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```
        "glue:ListSessions",
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCreateAndTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateSession",
        "glue:CreateBlueprint",
        "glue:CreateJob",
        "glue:CreateDataQualityRuleset",
        "glue:CreateWorkflow",
        "glue:TagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
```

```
      "Sid" : "GlueTagSessionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
      ],
      "Condition" : {
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GluePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:GetSession",
        "glue:ListStatements",
        "glue:DeleteSession",
        "glue:RunStatement",
        "glue:GetStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl",
```

```
        "glue:NotifyEvent",
        "glue:StartBlueprintRun",
        "glue:PutWorkflowRunProperties",
        "glue:DeleteJob",
        "glue:DeleteWorkflow",
        "glue:DeleteBlueprint",
        "glue:UpdateWorkflow",
        "glue:UpdateJob",
        "glue:StartWorkflowRun",
        "glue:ResumeWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:BatchStopJobRun",
        "glue:StopWorkflowRun",
        "glue:StartJobRun",
        "glue:CancelDataQualityRuleRecommendationRun",
        "glue:CancelDataQualityRulesetEvaluationRun",
        "glue:DeleteDataQualityRuleset",
        "glue:GetDataQualityModel",
        "glue:GetDataQualityModelResult",
        "glue:GetDataQualityResult",
        "glue:GetDataQualityRuleRecommendationRun",
        "glue:GetDataQualityRuleset",
        "glue:GetDataQualityRulesetEvaluationRun",
        "glue:ListDataQualityResults",
        "glue:ListDataQualityRuleRecommendationRuns",
        "glue:ListDataQualityRulesetEvaluationRuns",
        "glue:ListDataQualityRulesets",
        "glue:PublishDataQuality",
        "glue:PutDataQualityProfileAnnotation",
        "glue:PutDataQualityStatisticAnnotation",
        "glue:StartDataQualityRuleRecommendationRun",
        "glue:StartDataQualityRulesetEvaluationRun",
        "glue:UpdateDataQualityRuleset",
        "glue:GetJobRun",
        "glue:GetJobRuns",
        "glue:BatchGetJobs",
        "glue:GetJob"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*",
        "arn:aws:glue:*:*:blueprint/*",
        "arn:aws:glue:*:*:job/*",
        "arn:aws:glue:*:*:dataQualityRuleset/*",
        "arn:aws:glue:*:*:workflow/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueListJobsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListJobs"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:PrincipalTag/EnableGlueWorkloadsPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "GlueVisualETLPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetGeneratedCode"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueCompletionsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "glue:GetCompletion"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:completion/*",
        "arn:aws:glue:*:*:job/*"
      ]
    },
```

```
    {
      "Sid" : "GlueJobRunnerSessionLogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws-glue/*"
    },
    {
      "Sid" : "EC2TagsPermissionsForGlue",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DeleteTags",
        "ec2:CreateTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "aws-glue-*"
          ]
        },
        "StringEquals" : {
          "glue:RoleAssumedBy" : "glue.amazonaws.com",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : [
```

```
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/DefaultGlueCatalogKmsKeyId}",
        "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "glue.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "kms:EncryptionContext:glue_catalog_id" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessInteractivePermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:AccessInteractiveEndpoints",
        "emr-serverless:AccessLivyEndpoints",
        "emr-serverless:GetApplication",
        "emr-serverless:StartApplication",
        "emr-serverless:StopApplication"
      ],
      "Resource" : "arn:aws:emr-serverless:*:*:/applications/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EmrServerlessJobAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:GetDashboardForJobRun",
        "emr-serverless:GetJobRun"
      ],
      "Resource" : [
        "arn:aws:emr-serverless:*:*:/applications/*/jobruns/*"
      ],
      "Condition" : {
        "StringEquals" : {
```

```
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowActionsForTaggedEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:GetEnvironment",
        "airflow:UpdateEnvironment"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AirflowListEnvironments",
      "Effect" : "Allow",
      "Action" : [
        "airflow:ListEnvironments"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AirflowUiApiAccess",
      "Effect" : "Allow",
      "Action" : [
        "airflow:CreateWebLoginToken",
        "airflow:InvokeRestApi"
      ],
      "Resource" : [
        "arn:aws:airflow:*:*:role/DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}/User"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchLogsActions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:airflow-DataZoneMWAAEnv-${aws:PrincipalTag/
AmazonDataZoneDomain}-${aws:PrincipalTag/AmazonDataZoneProject}-${aws:PrincipalTag/
AmazonDataZoneScopeName}-*"
      ]
    },
    {
      "Sid" : "AirflowCloudwatchActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : "AmazonMWAA"
        }
      }
    },
    {
      "Sid" : "GlueJobCloudwatchPutMetricActions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "cloudwatch:namespace" : [
            "Glue",
            "AWS/Glue"
          ]
        }
      }
    },
```

```
    {
      "Sid" : "AirflowS3GetAccountPublicAccessBlock",
      "Effect" : "Allow",
      "Action" : "s3:GetAccountPublicAccessBlock",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowSqsActions",
      "Effect" : "Allow",
      "Action" : [
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:airflow-celery-*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketPublicAccessBlock"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "DataLakeS3BucketActions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketLocation"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountS3Permissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:GetPublicKey",
        "kms:DescribeKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
```

```
        }
      }
    },
    {
      "Sid" : "DataLakeCrossAccountDecryptKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:s3:arn"
        }
      }
    },
    {
      "Sid" : "ListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:ListBucketVersions"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringLike" : {
          "s3:prefix" : [
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}",
            "${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/
AmazonDataZoneProject}/*"
          ]
        },
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
```

```
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowListDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ListDomainBucketFromAthenaFederatedCatalog",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}"
      ],
      "Condition" : {
        "ArnEquals" : {
          "lambda:SourceFunctionArn" :
"arn:aws:lambda:*:*:function:athenafederatedcatalog_*"
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:GetObject*",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AccessLevelControlS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : "s3:GetBucketAcl",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "TagS3ObjectPermissionsForBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : "s3:PutObjectTagging",
      "Resource" : "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/
${aws:PrincipalTag/AmazonDataZoneDomain}/${aws:PrincipalTag/AmazonDataZoneProject}/
genAI/assets/evaluations/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/DomainBucketName" : "",
```

```
          "aws:PrincipalTag/AmazonDataZoneDomain" : "",
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        },
        "StringEquals" : {
          "s3:RequestObjectTag/BasicValidationStatus" : [
            "valid",
            "invalid"
          ],
          "s3:RequestObjectTag/ContainsReferenceResponseForAllPrompts" : [
            "true",
            "false"
          ]
        },
        "ForAllValues:StringEquals" : {
          "s3:RequestObjectTagKeys" : [
            "BasicValidationStatus",
            "ContainsReferenceResponseForAllPrompts"
          ]
        }
      }
    },
    {
      "Sid" : "AccessDomainS3BucketKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:aws:s3:arn" : [
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}",
            "arn:aws:s3:::${aws:PrincipalTag/DomainBucketName}/*"
          ]
        }
      }
    },
    {
      "Sid" : "DZDomainKMSKeyXAcctPerm",
      "Action" : [
```

```
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Effect" : "Allow",
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/DomainKmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "kms:EncryptionContext:aws:datazone:domainId" : "${aws:PrincipalTag/
AmazonDataZoneDomain}",
          "kms:ViaService" : [
            "datazone.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "ListLogGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueJobLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/output:log-
stream:*",
```

```
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}/error:log-
stream:*"
      ]
    },
    {
      "Sid" : "ProjectLogGroupPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetLogRecord",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}",
        "arn:aws:logs:*:*:log-group:${aws:PrincipalTag/LogGroupName}:log-stream:*"
      ]
    },
    {
      "Sid" : "CloudWatchStopQuery",
      "Effect" : "Allow",
      "Action" : [
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataLakeAthenaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:TerminateSession",
        "athena:CreatePreparedStatement",
        "athena:StopCalculationExecution",
        "athena:StartQueryExecution",
        "athena:UpdatePreparedStatement",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:UpdateNotebook",
```

```
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:UpdateNotebookMetadata",
        "athena:DeleteNamedQuery",
        "athena:GetCalculationExecution",
        "athena:GetCalculationExecutionCode",
        "athena:GetCalculationExecutionStatus",
        "athena:GetNamedQuery",
        "athena:GetNotebookMetadata",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetSession",
        "athena:GetSessionStatus",
        "athena:GetWorkGroup",
        "athena:UpdateNamedQuery",
        "athena:CreateNamedQuery",
        "athena:ExportNotebook",
        "athena:StopQueryExecution",
        "athena:StartCalculationExecution",
        "athena:StartSession",
        "athena:CreatePresignedNotebookUrl",
        "athena:CreateNotebook",
        "athena:ImportNotebook",
        "athena:ListQueryExecutions",
        "athena:ListTagsForResource",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "DefaultAthenaDataCatalogPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:GetDatabase",
```

```
        "athena:GetDataCatalog",
        "athena:GetTableMetadata",
        "athena:ListDatabases",
        "athena:ListTableMetadata"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:datacatalog/AwsDataCatalog",
        "arn:aws:athena:*:*:datacatalog/awsdatacatalog"
      ]
    },
    {
      "Sid" : "AthenaListPermissions",
      "Effect" : "Allow",
      "Action" : [
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListWorkGroups"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneUserPermissions",
      "Effect" : "Allow",
      "Action" : [
        "datazone:CreateConnection",
        "datazone:DeleteConnection",
        "datazone:GetConnection",
        "datazone:GetDomain",
        "datazone:GetDomainExecutionRoleCredentials",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentBlueprintConfiguration",
        "datazone:GetProject",
        "datazone:GetUserProfile",
        "datazone:ListConnections",
        "datazone:ListEnvironments",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListProjects",
        "datazone:UpdateConnection",
        "datazone:PostLineageEvent"
      ],
      "Resource" : "arn:aws:datazone:*:*:domain/${aws:PrincipalTag/
AmazonDataZoneDomain}"
    },
    {
```

```
      "Sid" : "GlueGetDefaultDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/default"
      ]
    },
    {
      "Sid" : "AllowGlueGetDatabasesExceptDefault",
      "Effect" : "Allow",
      "Action" : "glue:GetDatabases",
      "NotResource" : "arn:aws:glue:*:*:database/default",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueListDatabasesOnNoDatabases",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetDatabases"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueFileUploadPermissions",
      "Action" : [
        "glue:GetClassifier",
        "glue:GetClassifiers",
        "glue:UseGlueStudio"
      ],
      "Resource" : "*",
      "Effect" : "Allow"
    },
    {
      "Sid" : "GlueProjectConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:PassConnection",
```

```
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueGetConnectionOnlyOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections"
      ],
      "Resource" : "arn:aws:glue:*:*:catalog"
    },
    {
      "Sid" : "GlueDatalakePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateTable",
        "glue:DeleteTable",
        "glue:BatchDeleteTable",
        "glue:UpdateTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:DeletePartition",
        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:BatchGetPartition",
        "glue:BatchGetTableOptimizer",
        "glue:GetCatalogImportStatus",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetColumnStatisticsTaskRun",
        "glue:GetColumnStatisticsTaskRuns",
        "glue:GetDatabase",
        "glue:DeleteDatabase",
        "glue:GetPartition",
        "glue:GetPartitionIndexes",
```

```
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTableOptimizer",
        "glue:GetTableVersion",
        "glue:GetTableVersions",
        "glue:GetTables",
        "glue:SearchTables",
        "glue:ListTableOptimizerRuns",
        "glue:CreatePartitionIndex",
        "glue:BatchUpdatePartition",
        "glue:DeleteTableVersion",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartitionIndex",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:BatchDeleteTableVersion",
        "glue:GetCatalogs",
        "glue:GetCatalog"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueCrawlerPermissions",
      "Effect" : "Allow",
      "Action" : "glue:ListCrawls",
      "Resource" : "arn:aws:glue:*:*:crawler/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "GlueGlobalTempDatabasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
```

```
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/global_temp",
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GlueNonDefaultCatalogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetCatalog",
        "glue:UpdateCatalog"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GlueCatalogDatabasePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "glue:CreateDatabase",
        "glue:DeleteDatabase",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "LakeFormationPermissionForDataLakeAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataAccess",
        "lakeformation:GetResourceLFTags"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMListRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMGetRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:AssumeRole"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProject" : ""
        }
      }
    },
    {
      "Sid" : "SetSourceIdentityForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "TagSessionForAssumeAccessRole",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringEquals" : {
          "aws:TagKeys" : [
            "AmazonDataZoneProject",
            "AmazonDataZoneDomain"
          ]
        },
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:RequestTag/AmazonDataZoneDomain" : "${aws:PrincipalTag/
AmazonDataZoneDomain}"
        }
      }
    },
    {
      "Sid" : "SetContextForTrustedIdentityPropagation",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sts:SetContext"
      ],
      "Resource" : [
        "arn:aws:sts::*:self"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "sqlworkbench.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "StsContext",
      "Effect" : "Allow",
      "Action" : "sts:SetContext",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:ArnEquals" : {
          "sts:RequestContextProviders" : [
            "arn:aws:iam::aws:contextProvider/IdentityCenter"
          ]
        },
        "Null" : {
          "sts:RequestContextProviders" : "false"
        }
      }
    },
    {
      "Sid" : "FederatedDataConnectionPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "UnRestrictedAccessForGlueEntities",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListConnectionTypes",
        "glue:DescribeConnectionType"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueEntitiesAccessForFederatedDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:ListEntities",
        "glue:DescribeEntity",
        "glue:GetEntityRecords"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowPassRoleOnProjectRoles",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/RoleName}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "glue.amazonaws.com",
            "airflow.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "scheduler.amazonaws.com",
            "access-grants.s3.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "SQLWorkBenchActionsWithoutResourceType",
      "Effect" : "Allow",
```

```
      "Action" : [
        "sqlworkbench:PutTab",
        "sqlworkbench:DeleteTab",
        "sqlworkbench:DriverExecute",
        "sqlworkbench:GetUserInfo",
        "sqlworkbench:ListTabs",
        "sqlworkbench:GetAutocompletion*",
        "sqlworkbench:PassAccountSettings",
        "sqlworkbench:ListQueryExecutionHistory",
        "sqlworkbench:GetQueryExecutionHistory",
        "sqlworkbench:CreateConnection",
        "sqlworkbench:*QCustomContext",
        "sqlworkbench:GetQSql*",
        "sqlworkbench:GetSchemaInference"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBenchActions",
      "Effect" : "Allow",
      "Action" : "sqlworkbench:AssociateNotebookWithTab",
      "Resource" : "arn:*:sqlworkbench:*:*:notebook/*"
    },
    {
      "Sid" : "SQLWorkBenchNotebookActions",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:CreateNotebook*",
        "sqlworkbench:GetNotebook",
        "sqlworkbench:UpdateNotebook*",
        "sqlworkbench:DeleteNotebook*",
        "sqlworkbench:ExportNotebook",
        "sqlworkbench:BatchGetNotebookCell",
        "sqlworkbench:TagResource"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/sqlworkbench-resource-owner" : "${aws:userid}"
        }
      }
    },
```

```
    {
      "Sid" : "RedshiftDataActionsIAMSessionRestriction",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:ListStatements"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForResources",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AllowAccessExistingRedshiftCompute",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetCredentials",
        "redshift:DescribeTags",
```

```
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-data:BatchExecuteStatement",
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeTable",
        "redshift-data:ListDatabases",
        "redshift-data:ListSchemas",
        "redshift-data:ListTables"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        },
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneEnvironment" : "true"
        }
      }
    },
    {
      "Sid" : "RedshiftWithoutResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift:DescribeClusters"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftServerlessWorkgroupWithResourceType",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift:DescribeTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "RedshiftExistingComputeConnectToCatalog",
      "Effect" : "Allow",
      "Action" : [
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "arn:aws:redshift:*:*:dbname:*/*",
      "Condition" : {
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowListSecrets",
      "Effect" : "Allow",
      "Action" : "secretsmanager:ListSecrets",
      "Resource" : "*"
    },
    {
      "Sid" : "ComputeCredentials",
      "Effect" : "Allow",
      "Action" : [
        "emr-containers:DescribeManagedEndpoint",
        "emr-containers:DescribeSecurityConfiguration",
        "emr-containers:DescribeVirtualCluster",
        "emr-containers:GetManagedEndpointSessionCredentials",
        "redshift-serverless:GetCredentials",
        "redshift:GetClusterCredentialsWithIAM"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "RedshiftDataActionsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
```

```
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:CancelStatement",
        "redshift-data:GetStagingBucketLocation",
        "redshift-serverless:GetManagedWorkgroup"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "redshift-data:glue-catalog-arn" : "arn:aws:glue:*:*:catalog/*"
        }
      }
    },
    {
      "Sid" : "RedshifServerlessCredentialsForManagedWorkgroup",
      "Effect" : "Allow",
      "Action" : [
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "arn:aws:redshift-serverless:*:*:workgroup/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "redshift-data.amazonaws.com",
            "sqlworkbench.amazonaws.com"
          ]
        },
        "Bool" : {
          "aws:ViaAWSService" : "true"
        }
      }
    },
    {
      "Sid" : "AllowTagGetResources",
      "Effect" : "Allow",
      "Action" : "tag:GetResources",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:CalledViaLast" : "sqlworkbench.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid" : "AllowGetSecretForRedShift",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudWatchMetricsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonQChatPermissions",
      "Effect" : "Allow",
      "Action" : [
        "q:StartConversation",
        "q:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRClusterWithDataZoneTags",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:DescribeCluster",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListInstanceFleets",
        "elasticmapreduce:ListInstanceGroups",
        "elasticmapreduce:ListBootstrapActions",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:GetOnClusterAppUIPresignedURL"
```

```
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EMRClusterInfoPermissions",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:ListReleaseLabels",
        "elasticmapreduce:ListSupportedInstanceTypes",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:CreatePersistentAppUI",
        "elasticmapreduce:DescribePersistentAppUI",
        "pricing:GetProducts"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EMRGetClusterSessionCredentials",
      "Effect" : "Allow",
      "Action" : [
        "elasticmapreduce:GetClusterSessionCredentials"
      ],
      "Resource" : [
        "arn:aws:elasticmapreduce:*:*:cluster/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
```

```
    {
      "Sid" : "EmrContainersSSO",
      "Effect" : "Allow",
      "Action" : [
        "sso:DescribeApplication"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringLike" : {
          "aws:CalledVia" : [
            "emr-containers.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EMRPersistentAppUI",
      "Effect" : "Allow",
      "Resource" : "*",
      "Action" : [
        "elasticmapreduce:GetPersistentAppUIPresignedURL"
      ],
      "Condition" : {
        "ArnLike" : {
          "elasticmapreduce:ExecutionRoleArn" : "arn:aws:iam::*:role/
${aws:PrincipalTag/RoleName}"
        }
      }
    },
    {
      "Sid" : "KmsWithEncrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "bedrock.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "scheduler.*.amazonaws.com",
            "glue.*.amazonaws.com",
            "secretsmanager.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "EBDecrypt",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
```

```
        "StringLike" : {
          "kms:ViaService" : [
            "emr-serverless.*.amazonaws.com",
            "redshift.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "KmsManagement",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListGrants",
        "kms:RevokeGrant",
        "kms:DescribeKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com",
            "emr-serverless.*.amazonaws.com",
            "s3.*.amazonaws.com",
            "redshift.*.amazonaws.com",
            "codecommit.*.amazonaws.com",
            "scheduler.*.amazonaws.com"
          ]
        },
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsKeyPermissions",
      "Action" : [
        "kms:CreateGrant",
```

```
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "AwsOwnedKmsManagement",
      "Action" : [
        "kms:DescribeKey"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:kms:*:*:key/*"
      ],
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : [
            "sqs.*.amazonaws.com",
            "sagemaker.*.amazonaws.com"
          ]
        },
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    },
    {
      "Sid" : "ListKMS",
      "Effect" : "Allow",
      "Action" : [
        "kms:ListAliases"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "EC2PermissionsForNotebookExecution",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeInstanceTypes"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "InvokeBedrockModel",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        },
        "Null" : {
          "bedrock:InferenceProfileArn" : "false"
        }
      }
    },
```

```
    {
      "Sid" : "BedrockInvokeModelPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*:*:provisioned-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        },
        "ArnLike" : {
          "bedrock:InferenceProfileArn" : "arn:aws:bedrock:*:*:application-inference-
profile/*"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockInvokeModelAppInferenceProfilePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:GetInferenceProfile",
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource" : "arn:aws:bedrock:*:*:application-inference-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeAgent",
        "bedrock:Retrieve",
        "bedrock:ListIngestionJobs",
        "bedrock:StartIngestionJob",
        "bedrock:GetIngestionJob",
        "bedrock:ApplyGuardrail",
        "bedrock:ListPrompts",
        "bedrock:GetPrompt",
        "bedrock:CreatePrompt",
        "bedrock:DeletePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:InvokeFlow",
        "bedrock:GetEvaluationJob",
        "bedrock:CreateEvaluationJob",
        "bedrock:StopEvaluationJob",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:ListTagsForResource",
        "bedrock:CreateAgentAlias",
        "bedrock:ListAgentAliases",
        "bedrock:GetAgentVersion",
        "bedrock:ListAgentVersions",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:GetAgentAlias",
        "bedrock:UpdateAgentAlias"
      ],
      "Resource" : "*",
      "Condition" : {
```

```
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "BedrockResourceAccessPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ApplyGuardrail",
        "bedrock:BatchDeleteEvaluationJob",
        "bedrock:CreateAgentAlias",
        "bedrock:CreateBlueprint",
        "bedrock:CreateBlueprintVersion",
        "bedrock:CreateDataAutomationProject",
        "bedrock:CreateEvaluationJob",
        "bedrock:CreatePrompt",
        "bedrock:CreatePromptVersion",
        "bedrock:DeleteAgentAlias",
        "bedrock:DeleteAgentVersion",
        "bedrock:DeleteBlueprint",
        "bedrock:DeleteDataAutomationProject",
        "bedrock:DeletePrompt",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentVersion",
        "bedrock:GetBlueprint",
        "bedrock:GetDataAutomationProject",
        "bedrock:GetDataAutomationStatus",
        "bedrock:GetEvaluationJob",
        "bedrock:GetIngestionJob",
        "bedrock:GetPrompt",
        "bedrock:InvokeAgent",
        "bedrock:InvokeDataAutomationAsync",
        "bedrock:InvokeFlow",
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentVersions",
        "bedrock:ListIngestionJobs",
        "bedrock:ListPrompts",
        "bedrock:ListTagsForResource",
        "bedrock:Retrieve",
        "bedrock:StartIngestionJob",
        "bedrock:StopEvaluationJob",
```

```
        "bedrock:UpdateAgentAlias",
        "bedrock:UpdateBlueprint",
        "bedrock:UpdateDataAutomationProject",
        "bedrock:ListAgentActionGroups",
        "bedrock:ListAgentKnowledgeBases"
      ],
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateEvaluationJobForFoundationModelPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*::foundation-model/*",
        "arn:aws:bedrock:*:*:custom-model/*"
      ]
    },
    {
      "Sid" : "BedrockCreateEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:CreateEvaluationJob",
      "Resource" : [
        "arn:aws:bedrock:*:*:custom-model/*",
        "arn:aws:bedrock:*::foundation-model/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeDataAutomationAsyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:InvokeDataAutomationAsync"
      ],
```

```
      "Resource" : [
        "arn:aws:bedrock:*:*:data-automation-profile/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeBedrockInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockInvokeInlineAgentPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:InvokeInlineAgent",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "bedrock:InlineAgentName" : "${datazone:userId}"
        },
        "StringNotEquals" : {
          "bedrock:InlineAgentName" : ""
        }
      }
    },
    {
      "Sid" : "BedrockRetrieveAndGeneratePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:RetrieveAndGenerate",
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "ListBedrockEvaluationJobPermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:ListEvaluationJobs",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "BedrockNoResourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "bedrock:ListEvaluationJobs",
        "bedrock:RetrieveAndGenerate",
        "bedrock:ListFoundationModels"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true"
        }
      }
    },
    {
      "Sid" : "PassRoleToBedrockEvaluation",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
```

```
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "iam:PassedToService" : [
            "bedrock.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "IamPassRoleToBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/AmazonBedrockEvaluationRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*",
        "arn:aws:iam::*:role/AmazonBedrockServiceRole-${aws:PrincipalTag/
AmazonDataZoneProject}-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "iam:PassedToService" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "TagBedrockResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "AmazonBedrockManaged",
            "ProjectUserTag*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "BedrockTagResourcePermissions",
      "Effect" : "Allow",
      "Action" : "bedrock:TagResource",
      "Resource" : "arn:aws:bedrock:*:*:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonBedrockManaged",
            "AmazonDataZone*",
            "ProjectUserTag*"
          ]
        }
      }
    },
    {
      "Sid" : "BedrockKmsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
```

```
        "Null" : {
          "kms:EncryptionContext:aws:bedrock:arn" : "false"
        }
      }
    },
    {
      "Sid" : "KmsViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "ForAllValues:StringLike" : {
          "kms:EncryptionContextKeys" : [
            "aws:bedrock*:arn",
            "aws:bedrock:guardrail-id"
          ]
        }
      }
    },
    {
      "Sid" : "AccessSecretPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
```

```
    },
    {
      "Sid" : "SecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:DescribeSecret",
        "secretsmanager:PutSecretValue"
      ],
      "Resource" : "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "AccessSecretKmsPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock-ide/*"
        }
      }
    },
    {
      "Sid" : "KmsViaSecretsManagerPermissionsForBedrock",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "arn:aws:kms:*:*:key/${aws:PrincipalTag/KmsKeyId}",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "ArnLike" : {
          "kms:EncryptionContext:SecretARN" :
 "arn:aws:secretsmanager:*:*:secret:amazon-bedrock*"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAmazonBedrockIDE",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock-ide-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "LambdaInvokeFunctionViaBedrockPermissions",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:amazon-bedrock*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:CalledViaFirst" : "bedrock.amazonaws.com"
        }
      }
```

```
    },
    {
      "Sid" : "GetDataZoneEnvironmentCloudFormationStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:GetTemplate",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockIDEPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CloudFormationGetDataZoneEnvironmentStackPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/DataZone-Env-*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/EnableAmazonBedrockPermissions" : "true",
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}",
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "GetGlueUserDefinedFuncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetUserDefinedFunction",
        "glue:GetUserDefinedFunctions"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:userDefinedFunction/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionGetSecretPermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:GetSecretValue"
      ],
      "Resource" : "arn:*:secretsmanager:*:*:secret:*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionLambdaLogsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
```

```
      ],
      "Resource" : "arn:aws:logs:*:*:log-group:/aws/lambda/athenafederatedcatalog*"
    },
    {
      "Sid" : "FederatedConnectionDDBPermissions",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:ListTables"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConnectionEC2Permissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSubnets",
        "ec2:DetachNetworkInterface"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDeleteENIPermissions",
      "Effect" : "Allow",
      "Action" : "ec2:DeleteNetworkInterface",
      "Resource" : "arn:aws:ec2:*:*:*/*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ec2:Vpc" : "${aws:PrincipalTag/vpcArn}"
        }
      }
    },
    {
      "Sid" : "FederatedConnectionDescribeENIPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "PrivateECRPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:DeleteRepository",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:BatchDeleteImage",
        "ecr:ListTagsForResource",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecr:UploadLayerPart"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateECRRepositoryPermission",
      "Effect" : "Allow",
      "Action" : "ecr:CreateRepository",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "StringEquals" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRTagResourcePermission",
      "Effect" : "Allow",
      "Action" : "ecr:TagResource",
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
```

```
            "AmazonDataZoneProject",
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ECRUntagResourcePermission",
      "Effect" : "Allow",
      "Action" : [
        "ecr:UntagResource"
      ],
      "Resource" : "arn:aws:ecr:*:*:repository/*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*"
          ]
        },
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "LakeformationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:ListPermissions",
        "lakeformation:DescribeResource",
        "ram:GetResourceShareInvitations",
        "lakeformation:CreateDataCellsFilter",
        "lakeformation:ListDataCellsFilter",
```

```
        "lakeformation:DeleteDataCellsFilter",
        "lakeformation:GetDataCellsFilter",
        "lakeformation:UpdateDataCellsFilter",
        "ram:ListResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CrossAccountLakeFormationResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:CreateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "ram:RequestedResourceType" : [
            "glue:Table",
            "glue:Database",
            "glue:Catalog"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingPermissions",
      "Effect" : "Allow",
      "Action" : [
        "glue:DeleteResourcePolicy",
        "glue:PutResourcePolicy"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*",
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*"
      ],
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "aws:CalledVia" : [
            "ram.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:DeleteResourceShare",
        "ram:ListResourceSharePermissions",
        "ram:UpdateResourceShare"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*"
          ]
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "RAMGetResourceSharesViaLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "ram:GetResourceShares"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
```

```
    },
    {
      "Sid" : "CrossAccountRAMResourceShareInvitationPermission",
      "Effect" : "Allow",
      "Action" : [
        "ram:AcceptResourceShareInvitation"
      ],
      "Resource" : "arn:aws:ram:*:*:resource-share-invitation/*",
      "Condition" : {
        "StringLike" : {
          "ram:ResourceShareName" : [
            "LakeFormation*",
            "DataZoneS3AG*"
          ]
        }
      }
    },
    {
      "Sid" : "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
      "Effect" : "Allow",
      "Action" : "ram:AssociateResourceSharePermission",
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "ram:PermissionArn" : "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
        },
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:GetSchedule",
        "scheduler:UpdateSchedule",
        "scheduler:DeleteSchedule"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule/*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "EventBridgeScheduleGroupActions",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:GetScheduleGroup"
      ],
      "Resource" : [
        "arn:aws:scheduler:*:*:schedule-group/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageQuickSightFolderAndDataSourceResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSource",
        "quicksight:DescribeFolder",
        "quicksight:DescribeFolderPermissions",
        "quicksight:ListFolderMembers"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:folder/*",
        "arn:aws:quicksight:*:*:datasource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
```

```
    {
      "Sid" : "ManageQuickSightOtherResources",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:DescribeDataSet",
        "quicksight:DescribeAccountSubscription",
        "quicksight:DescribeUser",
        "quicksight:DescribeGroup"
      ],
      "Resource" : [
        "arn:aws:quicksight:*:*:*"
      ]
    },
    {
      "Sid" : "ManagePassDataSourcePermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:PassDataSource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:datasource/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "ManageCreateDataSetPermissions",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateDataSet",
        "quicksight:TagResource"
      ],
      "Resource" : "arn:aws:quicksight:*:*:dataset/*",
      "Condition" : {
        "Null" : {
          "aws:TagKeys" : "false"
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        },
```

```
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        },
        "StringEqualsIfExists" : {
          "aws:RequestTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}"
        }
      }
    },
    {
      "Sid" : "CreateFolderMembership",
      "Effect" : "Allow",
      "Action" : [
        "quicksight:CreateFolderMembership"
      ],
      "Resource" : "arn:aws:quicksight:*:*:folder/sagemaker-*-assets",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${aws:PrincipalTag/
AmazonDataZoneProject}",
          "aws:ResourceTag/AmazonDataZoneAssetsFolder" : "true"
        }
      }
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen

- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioQueryExecutionRolePolicy

Beschreibung: Amazon SageMaker Studio verwendet diese Richtlinie, wenn Abfrageausführungen auf Verbundverbindungen ausgeführt werden.

`SageMakerStudioQueryExecutionRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioQueryExecutionRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 31. Januar 2025, 19:52 UTC
- Bearbeitete Zeit: 4. September 2025, 17:49 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SageMakerStudioQueryExecutionRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "GlueGetConnectionOnCatalog",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:catalog"
      ]
    },
    {
      "Sid" : "GlueGetConnectionsForProject",
      "Effect" : "Allow",
      "Action" : [
        "glue:GetConnection",
        "glue:GetConnections",
        "glue:GetTags"
      ],
      "Resource" : "arn:aws:glue:*:*:connection/*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "false"
        }
      }
    },
    {
      "Sid" : "S3GetObjectForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::*/dzd*/*/dev/sys/athena/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "S3ListBucketOwnershipCheckForAthenaSpillBucket",
      "Effect" : "Allow",
      "Action" : [
```

```
        "s3:ListBucket"
      ],
      "Resource" : [
        "arn:aws:s3:::amazon-sagemaker-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true"
        }
      }
    },
    {
      "Sid" : "InvokeFunctionPermissionsForAthenaCatalogLambda",
      "Effect" : "Allow",
      "Action" : "lambda:InvokeFunction",
      "Resource" : "arn:aws:lambda:*:*:function:*",
      "Condition" : {
        "StringEquals" : {
          "aws:PrincipalTag/SageMakerStudioQueryExecutionRole" : "true",
          "aws:ResourceTag/federated_athena_datacatalog" : "true"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioUserIAMConsolePolicy

Beschreibung: Bietet individuelle Einrichtungsrechte für Amazon SageMaker Unified Studio über das AWS-Managementkonsole und SDK. Ermöglicht das Starten des SageMaker Unified Studio-Portals.

`SageMakerStudioUserIAMConsolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioUserIAMConsolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 22:49 UTC
- Bearbeitete Zeit: 14. November 2025, 22:49 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMConsolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AmazonDataZoneStatement",
      "Effect" : "Allow",
      "Action" : [
        "datazone:ListDomains",
        "datazone:GetDomain",
        "datazone:GetUserProfile",
        "datazone:ListProjects",
        "datazone:ListProjectProfiles",
        "datazone:CreateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:GetIamPortalLoginUrl",
        "datazone:ListEnvironmentBlueprints",
```

```
        "datazone:ListEnvironments",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetGroupProfile",
        "datazone:SearchGroupProfiles",
        "datazone:SearchUserProfiles",
        "datazone:ListProjectMemberships"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "ReadOnlyStatement",
      "Effect" : "Allow",
      "Action" : [
        "iam:ListRoles",
        "iam:GetRole",
        "iam:GetUser"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DataZoneKMSPermissions",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioUserIAMDefaultExecutionPolicy

Beschreibung: Ausführungsrichtlinie für die Verwendung von IAM-Rollen mit SageMaker Unified Studio. Ermöglicht Benutzern den Zugriff auf Ressourcen im lokalen Konto (mit Ausnahme des Zugriffs auf Datenressourcen) für die IAM-basierte Nutzung von SageMaker Unified Studio.

`SageMakerStudioUserIAMDefaultExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioUserIAMDefaultExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 17:19 UTC
- Bearbeitete Zeit: 18. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMDefaultExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v6 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
```

```
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerUnifiedStudioMcp",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker-unified-studio-mcp:InvokeMcp",
        "sagemaker-unified-studio-mcp:CallReadOnlyTool",
```

```
        "sagemaker-unified-studio-mcp:CallPrivilegedTool"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
```

```
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "Q",
      "Effect" : "Allow",
      "Action" : [
        "glue:StartCompletion",
        "q:Get*",
        "q:List*",
        "q:PassRequest",
        "q:SendMessage",
        "q:StartConversation"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
```

```
    {
      "Sid" : "SageMakerUserTagPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreatePresignedDomainUrl",
        "sagemaker:CreateUserProfile",
        "sagemaker:DeleteUserProfile"
      ],
      "Resource" : "arn:aws:sagemaker:*:*:user-profile/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SageMakerPrivateSpace",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:CreateApp",
        "sagemaker:CreateSpace",
        "sagemaker:DeleteApp",
        "sagemaker:DeleteSpace",
        "sagemaker:UpdateSpace"
      ],
      "Resource" : [
        "arn:aws:sagemaker:*:*:space/*",
        "arn:aws:sagemaker:*:*:app/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}",
          "sagemaker:SpaceSharingType" : [
            "Private"
          ]
        }
      }
    },
    {
      "Sid" : "AllowStartSessionForSpaceRemoteConnection",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:StartSession"
      ],
```

```
      "Resource" : "arn:aws:sagemaker:*:*:space/*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneUser" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "ResourceGroupsPermissions",
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerPermissions",
      "Effect" : "Allow",
      "Action" : [
        "sagemaker:Batch*",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sagemaker:Search",
        "sagemaker:*Endpoint*",
        "sagemaker:*Model*",
        "sagemaker:*Context*",
        "sagemaker:*Artifact*",
        "sagemaker:*Action*",
        "sagemaker:*Association*",
        "sagemaker:QueryLineage",
        "sagemaker:*InferenceComponent*",
        "sagemaker:*Job*",
        "sagemaker:StartMlflowTrackingServer",
        "sagemaker:StopMlflowTrackingServer",
        "sagemaker:CreatePresignedMlflowTrackingServerUrl",
        "sagemaker-mlflow:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SageMakerTagPermissions",
      "Effect" : "Allow",
      "Action" : [
```

```
        "sagemaker:AddTags",
        "sagemaker:DeleteTags"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringNotLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*",
            "sagemaker:shared-with:*"
          ]
        },
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "ProjectUserTag*",
            "sagemaker*",
            "sm-jumpstart*",
            "endpoint-has-jumpstart-model"
          ]
        }
      }
    },
    {
      "Sid" : "LogsAndMetrics",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:PutMetricData",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:Describe*",
        "logs:Get*",
        "logs:PutLogEvents",
        "logs:StopQuery"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Glue",
      "Effect" : "Allow",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:CreateCatalog",
        "glue:Describe*",
```

```
        "glue:Get*",
        "glue:List*",
        "glue:NotifyEvent",
        "glue:RunStatement",
        "glue:StartCompletion",
        "glue:StopSession",
        "glue:UseGlueStudio",
        "glue:TagResource",
        "glue:UntagResource",
        "glue:*Job*",
        "glue:TestConnection"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
```

```
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "GlueDatabase",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:database/*",
        "arn:aws:glue:*:*:table/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:catalog/*"
      ]
    },
    {
      "Sid" : "GlueLakeFormation",
      "Effect" : "Allow",
      "Action" : [
        "glue:*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "glue:LakeFormationPermissions" : "Enabled"
        }
      }
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
```

```
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SQLWorkBench",
      "Effect" : "Allow",
      "Action" : [
        "sqlworkbench:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "RedshiftData",
      "Effect" : "Allow",
      "Action" : "redshift-data:*",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "redshift-data:statement-owner-iam-userid" : "${aws:userid}"
        }
      }
    },
    {
      "Sid" : "RedShiftActions",
      "Effect" : "Allow",
      "Action" : [
        "redshift-data:BatchExecuteStatement",
        "redshift-data:Describe*",
        "redshift-data:ExecuteStatement",
        "redshift-data:List*",
        "redshift-serverless:GetManagedWorkgroup",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:List*",
        "redshift:Describe*",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift-serverless:GetCredentials"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Bedrock",
      "Effect" : "Allow",
```

```
      "Action" : "bedrock:*",
      "Resource" : "*"
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : [
        "iam:PassRole"
      ],
      "Resource" : "arn:aws:iam::*:role/${aws:PrincipalTag/
AmazonDataZonePassedRolePath}",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "bedrock.amazonaws.com",
            "glue.amazonaws.com",
            "lakeformation.amazonaws.com",
            "sagemaker.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ],
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AirflowServerless",
      "Effect" : "Allow",
      "Action" : [
        "airflow-serverless:List*",
        "airflow-serverless:Get*",
        "airflow-serverless:CreateWorkflow",
        "airflow-serverless:UpdateWorkflow",
        "airflow-serverless:DeleteWorkflow",
        "airflow-serverless:StartWorkflowRun",
        "airflow-serverless:StopWorkflowRun",
        "airflow-serverless:TagResource",
        "airflow-serverless:UntagResource"
      ],
      "Resource" : "*"
    },
    {
```

```
      "Sid" : "S3List",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetBucketAcl",
        "s3:List*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3CrossAccount",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "Scheduler",
      "Effect" : "Allow",
      "Action" : [
        "scheduler:CreateSchedule",
        "scheduler:DeleteSchedule",
        "scheduler:Get*",
        "scheduler:List*",
        "scheduler:UpdateSchedule"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets"
      ],
```

```
      "Resource" : "*"
    },
    {
      "Sid" : "Athena",
      "Effect" : "Allow",
      "Action" : [
        "athena:BatchGet*",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:Get*",
        "athena:ImportNotebook",
        "athena:List*",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TagResource",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
```

```
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
```

```
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "GenerateRecommendations",
      "Effect" : "Allow",
      "Action" : [
        "codewhisperer:GenerateRecommendations"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
```

```
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
```

```
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
```

```
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
```

```
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AccessProjectS3BucketPermissions",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject*",
        "s3:PutObject*",
        "s3:RestoreObject",
        "s3:ReplicateObject",
        "s3:DeleteObject*",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
```

```
      "Resource" : [
        "arn:aws:s3:::${aws:PrincipalTag/AmazonDataZoneProjectBucket}/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:PrincipalTag/AmazonDataZoneProjectBucket" : ""
        }
      }
    },
    {
      "Sid" : "EMRServerless",
      "Effect" : "Allow",
      "Action" : [
        "emr-serverless:ListApplications",
        "emr-serverless:GetApplication"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SageMakerStudioUserIAMPermissiveExecutionPolicy

Beschreibung: Ausführungsrichtlinie für die Verwendung von IAM-Rollen mit SageMaker Unified Studio. Ermöglicht Benutzern den Zugriff auf Ressourcen in Ihrem Konto (einschließlich umfassendem Zugriff auf APIs All-In-Datendienste wie S3, Glue, CloudWatch Logs und andere) für die IAM-basierte Nutzung von SageMaker Unified Studio.

`SageMakerStudioUserIAMPermissiveExecutionPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SageMakerStudioUserIAMPermissiveExecutionPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 18. August 2025, 17:19 Uhr UTC
- Bearbeitete Zeit: 18. November 2025, 23:34 UTC
- ARN: `arn:aws:iam::aws:policy/SageMakerStudioUserIAMPermissiveExecutionPolicy`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "DataAccess",
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:*",
        "glue:*",
        "logs:*",
        "redshift-data:*",
        "redshift-serverless:*",
        "redshift:*",
        "s3:*"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "ComputeAccess",
      "Effect" : "Allow",
      "Action" : [
        "athena:*",
        "bedrock:*",
        "codewhisperer:*",
        "sagemaker-unified-studio-mcp:*",
        "q:*",
        "sagemaker:*",
        "sagemaker-mlflow:*",
        "scheduler:*",
        "sqlworkbench:*",
        "emr-serverless:*",
        "airflow-serverless:*"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "GlueSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "glue:CancelStatement",
        "glue:CreateSession",
        "glue:DeleteSession",
        "glue:GetSession",
        "glue:GetStatement",
        "glue:RunStatement",
        "glue:StopSession",
        "glue:GetDashboardUrl"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignSessions",
```

```
      "Effect" : "Deny",
      "Action" : [
        "glue:TagResource",
        "glue:UntagResource"
      ],
      "Resource" : "arn:aws:glue:*:*:session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DataZone",
      "Effect" : "Allow",
      "Action" : [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelMetadataGenerationRun",
        "datazone:CancelSubscription",
        "datazone:CreateAsset*",
        "datazone:CreateConnection",
        "datazone:CreateEnvironment",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset*",
        "datazone:DeleteConnection",
        "datazone:DeleteEnvironment",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:Get*",
        "datazone:List*",
        "datazone:PostLineageEvent",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchListings",
        "datazone:SearchRules",
        "datazone:SearchTypes",
```

```
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:StartMetadataGenerationRun",
        "datazone:UpdateAssetFilter",
        "datazone:UpdateConnection",
        "datazone:UpdateEnvironment",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionRequest",
        "datazone:CreateNotebook",
        "datazone:UpdateNotebook",
        "datazone:DeleteNotebook",
        "datazone:CreateCell",
        "datazone:UpdateCell",
        "datazone:DeleteCell",
        "datazone:BatchGetCell",
        "datazone:CreateCellRun",
        "datazone:UpdateCellRun",
        "datazone:DeleteCellRun",
        "datazone:BatchGetCellRun",
        "datazone:PutCellRunResult",
        "datazone:StartNotebookCompute",
        "datazone:StopNotebookCompute",
        "datazone:StartConversation",
        "datazone:GenerateCode",
        "datazone:SendMessage"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CfnManage",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:*"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stack/DataZone*"
      ]
    },
    {
      "Sid" : "ValidateCfn",
      "Effect" : "Allow",
      "Action" : "cloudformation:ValidateTemplate",
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "IamSts",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "sts:AssumeRole"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/neptune-graph.amazonaws.com/
AWSServiceRoleForNeptuneGraph",
        "arn:aws:iam::*:role/aws-service-role/redshift.amazonaws.com/
AWSServiceRoleForRedshift",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks",
        "arn:aws:iam::*:role/aws-service-role/ops.emr-serverless.amazonaws.com/
AWSServiceRoleForAmazonEMRServerless",
        "arn:aws:iam::*:role/aws-service-role/airflow.amazonaws.com/
AWSServiceRoleForAmazonMWAA",
        "arn:aws:iam::*:role/aws-service-role/airflow-serverless.amazonaws.com/
AWSServiceRoleForAmazonMWAAServerless",
        "arn:aws:iam::*:role/aws-service-role/elasticmapreduce.amazonaws.com/
AWSServiceRoleForEMRCleanup",
        "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
        "arn:aws:iam::*:role/aws-service-role/observability.aoss.amazonaws.com/
AWSServiceRoleForAmazonOpenSearchServerless"
      ]
    },
    {
      "Sid" : "TagSession",
      "Effect" : "Allow",
      "Action" : "sts:TagSession",
      "Resource" : "*",
      "Condition" : {
        "ForAllValues:StringLike" : {
          "aws:TagKeys" : [
            "AmazonDataZone*"
```

```
          ]
        }
      }
    },
    {
      "Sid" : "PassRole",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : [
        "arn:aws:iam::*:role/service-role/AmazonSageMaker*"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : [
            "sagemaker.amazonaws.com",
            "lakeformation.amazonaws.com",
            "glue.amazonaws.com",
            "bedrock.amazonaws.com",
            "redshift-serverless.amazonaws.com",
            "redshift.amazonaws.com",
            "scheduler.amazonaws.com",
            "emr-serverless.amazonaws.com",
            "airflow-serverless.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "SourceIdentity",
      "Effect" : "Allow",
      "Action" : "sts:SetSourceIdentity",
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "sts:SourceIdentity" : "${aws:PrincipalTag/datazone:userId}"
        }
      }
    },
    {
      "Sid" : "SSM",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetParameter*"
      ],
```

```
      "Resource" : [
        "arn:aws:ssm:*:*:parameter/amazon/datazone/q*",
        "arn:aws:ssm:*:*:parameter/amazon/datazone/genAI/*",
        "arn:aws:ssm:*::parameter/aws/service/sagemaker-distribution/*"
      ]
    },
    {
      "Sid" : "LFAccess",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:BatchGrantPermissions",
        "lakeformation:BatchRevokePermissions",
        "lakeformation:DescribeResource",
        "lakeformation:GetDataAccess",
        "lakeformation:GrantPermissions",
        "lakeformation:ListResources",
        "lakeformation:ListPermissions",
        "lakeformation:RevokePermissions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "FederatedConn",
      "Effect" : "Allow",
      "Action" : [
        "dynamodb:List*",
        "dynamodb:Describe*",
        "dynamodb:Scan",
        "dynamodb:PartiQLSelect",
        "dynamodb:Query",
        "secretsmanager:ListSecrets",
        "resource-groups:GetGroupQuery",
        "resource-groups:ListGroupResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "PrivateSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
```

```
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutResourcePolicy"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/AmazonDataZoneProject" : "${datazone:projectId}"
        }
      }
    },
    {
      "Sid" : "SharedSecret",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:CreateSecret",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetSecretValue",
        "secretsmanager:UpdateSecret"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceTag/for-use-with-all-datazone-projects" : "true"
        }
      }
    },
    {
      "Sid" : "Ecr",
      "Effect" : "Allow",
      "Action" : [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:DescribeImages",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "CodeConnectionsUser",
      "Effect" : "Allow",
      "Action" : [
        "codeconnections:UseConnection",
        "codeconnections:ListConnections",
```

```
        "codeconnections:GetConnection",
        "codeconnections:GetHost",
        "codeconnections:ListTagsForResource",
        "codestar-connections:UseConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:GetConnection",
        "codestar-connections:GetHost",
        "codestar-connections:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsListAndDescribe",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListGrants"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DataZoneKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:datazone:domainId"
        }
      }
    },
    {
      "Sid" : "S3Kms",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "s3.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:aws:s3:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SchedulerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "kms:EncryptionContext:aws:scheduler:schedule:arn" : "false"
        }
      }
    },
    {
      "Sid" : "SecretsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "secretsmanager.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContext:SecretARN" : "false"
```

```
        }
      }
    },
    {
      "Sid" : "SageMakerKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "SageMakerCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "sagemaker.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "DataZoneCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "datazone.*.amazonaws.com"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Encrypt",
            "Decrypt",
            "ReEncryptFrom",
            "ReEncryptTo",
            "GenerateDataKeyWithoutPlaintext",
            "GenerateDataKey",
            "DescribeKey",
            "RetireGrant",
            "CreateGrant"
          ]
        }
      }
    },
    {
      "Sid" : "GlueKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "glue.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "BedrockKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant",
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "bedrock.*.amazonaws.com"
        },
        "Null" : {
          "kms:EncryptionContextKeys" : "false"
        }
      }
    },
    {
      "Sid" : "WorkflowsCreateGrant",
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "StringLike" : {
          "kms:ViaService" : "airflow-serverless.*.amazonaws.com"
        },
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        },
        "ForAllValues:StringEquals" : {
          "kms:GrantOperations" : [
            "Decrypt",
            "Encrypt",
            "GenerateDataKey",
            "GenerateDataKeyWithoutPlaintext",
            "RetireGrant"
          ]
        }
      }
    },
    {
      "Sid" : "WorkflowsKms",
      "Effect" : "Allow",
      "Action" : [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
```

```
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource" : "arn:*:kms:*:*:key/*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "kms:EncryptionContextKeys" : "aws:airflow-serverless:workflow-arn"
        }
      }
    },
    {
      "Sid" : "Ec2DescribeOnly",
      "Effect" : "Allow",
      "Action" : "ec2:Describe*",
      "Resource" : "*"
    },
    {
      "Sid" : "VpcAccess",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "EC2TagAccessForVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource" : [
        "arn:aws:ec2:*:*:network-interface/*"
      ]
    },
    {
      "Sid" : "AthenaSessionIsolation",
      "Effect" : "Deny",
      "Action" : [
        "athena:StartSession",
        "athena:GetSession",
        "athena:TerminateSession",
```

```
        "athena:GetSessionStatus",
        "athena:GetSessionEndpoint",
        "athena:GetResourceDashboard"
      ],
      "Resource" : [
        "arn:aws:athena:*:*:workgroup/*/session/*"
      ],
      "Condition" : {
        "StringNotEquals" : {
          "aws:RequestTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}",
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    },
    {
      "Sid" : "DenyTaggingUntaggingForeignAthenaSessions",
      "Effect" : "Deny",
      "Action" : [
        "athena:TagResource",
        "athena:UntagResource"
      ],
      "Resource" : "arn:aws:athena:*:*:workgroup/*/session/*",
      "Condition" : {
        "StringNotEquals" : {
          "aws:ResourceTag/AmazonDataZoneSessionOwner" : "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecretsManagerReadWrite

Beschreibung: Ermöglicht read/write den Zugriff auf AWS Secrets Manager über die AWS-Managementkonsole. Hinweis: Dies schließt IAM-Aktionen aus. Kombinieren Sie es daher mit IAMFull Access, wenn eine Rotationskonfiguration erforderlich ist.

`SecretsManagerReadWrite`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `SecretsManagerReadWrite` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 4. April 2018, 18:05 UTC
- Bearbeitete Zeit: 22. Februar 2024, 18:12 UTC
- ARN: `arn:aws:iam::aws:policy/SecretsManagerReadWrite`

Version der Richtlinie

Richtlinienversion: v5 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BasePermissions",
      "Effect" : "Allow",
      "Action" : [
        "secretsmanager:*",
        "cloudformation:CreateChangeSet",
        "cloudformation:DescribeChangeSet",
```

```
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:ExecuteChangeSet",
        "docdb-elastic:GetCluster",
        "docdb-elastic:ListClusters",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "kms:DescribeKey",
        "kms:ListAliases",
        "kms:ListKeys",
        "lambda:ListFunctions",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "tag:GetResources"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LambdaPermissions",
      "Effect" : "Allow",
      "Action" : [
        "lambda:AddPermission",
        "lambda:CreateFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:SecretsManager*"
    },
    {
      "Sid" : "SARPermissions",
      "Effect" : "Allow",
      "Action" : [
        "serverlessrepo:CreateCloudFormationChangeSet",
        "serverlessrepo:GetApplication"
      ],
      "Resource" : "arn:aws:serverlessrepo:*:*:applications/SecretsManager*"
    },
    {
      "Sid" : "S3Permissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::awsserverlessrepo-changesets*",
        "arn:aws:s3:::secrets-manager-rotation-apps-*/*"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityAgentWebAppAPIPolicy

Beschreibung: Ermöglicht authentifizierten Benutzern den Zugriff auf die Security Agent Webanwendung zur Konfiguration und Ausführung automatisierter Sicherheits-Penetrationstests. Diese Richtlinie ermöglicht es Benutzern, Pentests zu verwalten, Ergebnisse einzusehen, die Testausführung zu überwachen und mit AWS Ressourcen zu interagieren, die für Sicherheitstests erforderlich sind.

`SecurityAgentWebAppAPIPolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SecurityAgentWebAppAPIPolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 02. Dezember 2025, 15:04 Uhr UTC

- Bearbeitete Zeit: 10. Dezember 2025, 01:04 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/SecurityAgentWebAppAPIPolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ApplicationAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:ListAgentInstances",
        "securityagent:ListControls"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AgentInstanceAccess",
      "Effect" : "Allow",
      "Action" : [
        "securityagent:AddArtifact",
        "securityagent:BatchDeletePentests",
        "securityagent:BatchGetAgentInstances",
        "securityagent:BatchGetArtifactMetadata",
        "securityagent:BatchGetFindings",
        "securityagent:BatchGetPentestJobs",
```

```
        "securityagent:BatchGetPentests",
        "securityagent:BatchGetSecurityTestContentMetadata",
        "securityagent:BatchGetTasks",
        "securityagent:CreateDocumentReview",
        "securityagent:CreatePentest",
        "securityagent:DeleteArtifact",
        "securityagent:GetArtifact",
        "securityagent:GetCodeReviewTask",
        "securityagent:GetDocReviewTask",
        "securityagent:GetDocumentReview",
        "securityagent:GetDocumentReviewArtifact",
        "securityagent:ListArtifacts",
        "securityagent:ListControls",
        "securityagent:ListDiscoveredEndpoints",
        "securityagent:ListDocumentReviewComments",
        "securityagent:ListDocumentReviews",
        "securityagent:ListFindings",
        "securityagent:ListIntegratedResources",
        "securityagent:ListPentestJobsForPentest",
        "securityagent:ListPentests",
        "securityagent:ListTasks",
        "securityagent:StartPentestExecution",
        "securityagent:StopPentestExecution",
        "securityagent:UpdateFinding",
        "securityagent:UpdatePentest"
      ],
      "Resource" : "arn:aws:securityagent:*:*:agent-instance*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityAudit

Beschreibung: Die Vorlage für die Sicherheitsüberprüfung gewährt Zugriff auf lesbare Metadaten zur Sicherheitskonfiguration. Es ist nützlich für Software, die die Konfiguration eines überprüft AWS-Konto.

`SecurityAudit`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SecurityAudit` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 13. Oktober 2025, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/SecurityAudit`

Version der Richtlinie

Richtlinienversion: v56 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "BaseSecurityAuditStatement",
      "Effect" : "Allow",
```

```
      "Action" : [
        "a4b:ListSkills",
        "access-analyzer:GetAnalyzedResource",
        "access-analyzer:GetAnalyzer",
        "access-analyzer:GetArchiveRule",
        "access-analyzer:GetFinding",
        "access-analyzer:ListAnalyzedResources",
        "access-analyzer:ListAnalyzers",
        "access-analyzer:ListArchiveRules",
        "access-analyzer:ListFindings",
        "access-analyzer:ListTagsForResource",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetPrimaryEmail",
        "account:GetRegionOptStatus",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:DescribeCertificateAuthorityAuditReport",
        "acm-pca:GetPolicy",
        "acm-pca:ListCertificateAuthorities",
        "acm-pca:ListPermissions",
        "acm-pca:ListTags",
        "acm:Describe*",
        "acm:List*",
        "airflow:GetEnvironment",
        "airflow:ListEnvironments",
        "appflow:ListFlows",
        "appflow:ListTagsForResource",
        "application-autoscaling:Describe*",
        "appmesh:Describe*",
        "appmesh:List*",
        "apprunner:DescribeAutoScalingConfiguration",
        "apprunner:DescribeCustomDomains",
        "apprunner:DescribeObservabilityConfiguration",
        "apprunner:DescribeService",
        "apprunner:DescribeVpcConnector",
        "apprunner:DescribeVpcIngressConnection",
        "apprunner:ListAutoScalingConfigurations",
        "apprunner:ListConnections",
        "apprunner:ListObservabilityConfigurations",
        "apprunner:ListOperations",
        "apprunner:ListServices",
        "apprunner:ListTagsForResource",
        "apprunner:ListVpcConnectors",
        "apprunner:ListVpcIngressConnections",
```

```
        "appsync:GetApiCache",
        "appsync:List*",
        "athena:GetWorkGroup",
        "athena:List*",
        "auditmanager:GetAccountStatus",
        "auditmanager:ListAssessmentControlInsightsByControlDomain",
        "auditmanager:ListAssessmentFrameworks",
        "auditmanager:ListAssessmentFrameworkShareRequests",
        "auditmanager:ListAssessmentReports",
        "auditmanager:ListAssessments",
        "auditmanager:ListControlDomainInsights",
        "auditmanager:ListControlDomainInsightsByAssessment",
        "auditmanager:ListControlInsightsByControlDomain",
        "auditmanager:ListControls",
        "auditmanager:ListNotifications",
        "auditmanager:ListTagsForResource",
        "autoscaling-plans:DescribeScalingPlans",
        "autoscaling:Describe*",
        "backup:DescribeGlobalSettings",
        "backup:DescribeRegionSettings",
        "backup:GetBackupVaultAccessPolicy",
        "backup:GetBackupVaultNotifications",
        "backup:ListBackupVaults",
        "backup:ListTags",
        "batch:DescribeComputeEnvironments",
        "batch:DescribeJobDefinitions",
        "bedrock:GetAgentAlias",
        "bedrock:GetAgentKnowledgeBase",
        "bedrock:GetCustomModel",
        "bedrock:GetFlowAlias",
        "bedrock:GetFoundationModel",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetImportedModel",
        "bedrock:GetInferenceProfile",
        "bedrock:GetIngestionJob",
        "bedrock:GetKnowledgeBaseDocuments",
        "bedrock:GetMarketplaceModelEndpoint",
        "bedrock:GetModelCopyJob",
        "bedrock:GetModelCustomizationJob",
        "bedrock:GetModelImportJob",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:GetPromptRouter",
        "bedrock:GetProvisionedModelThroughput",
        "bedrock:ListAgentActionGroups",
```

```
        "bedrock:ListAgentAliases",
        "bedrock:ListAgentKnowledgeBases",
        "bedrock:ListAgents",
        "bedrock:ListAgentVersions",
        "bedrock:ListCustomModels",
        "bedrock:ListDataSources",
        "bedrock:ListEvaluationJobs",
        "bedrock:ListFlowAliases",
        "bedrock:ListFlows",
        "bedrock:ListFlowVersions",
        "bedrock:ListFoundationModels",
        "bedrock:ListGuardrails",
        "bedrock:ListImportedModels",
        "bedrock:ListInferenceProfiles",
        "bedrock:ListIngestionJobs",
        "bedrock:ListKnowledgeBases",
        "bedrock:ListMarketplaceModelEndpoints",
        "bedrock:ListModelCopyJobs",
        "bedrock:ListModelCustomizationJobs",
        "bedrock:ListModelImportJobs",
        "bedrock:ListModelInvocationJobs",
        "bedrock:ListPromptRouters",
        "bedrock:ListPrompts",
        "bedrock:ListProvisionedModelThroughputs",
        "bedrock:ListTagsForResource",
        "braket:SearchJobs",
        "braket:SearchQuantumTasks",
        "chime:List*",
        "cleanrooms:BatchGetCollaborationAnalysisTemplate",
        "cleanrooms:BatchGetSchema",
        "cleanrooms:BatchGetSchemaAnalysisRule",
        "cleanrooms:GetAnalysisTemplate",
        "cleanrooms:GetCollaboration",
        "cleanrooms:GetCollaborationAnalysisTemplate",
        "cleanrooms:GetCollaborationConfiguredAudienceModelAssociation",
        "cleanrooms:GetCollaborationIdNamespaceAssociation",
        "cleanrooms:GetCollaborationPrivacyBudgetTemplate",
        "cleanrooms:GetConfiguredAudienceModelAssociation",
        "cleanrooms:GetConfiguredTable",
        "cleanrooms:GetConfiguredTableAnalysisRule",
        "cleanrooms:GetConfiguredTableAssociation",
        "cleanrooms:GetConfiguredTableAssociationAnalysisRule",
        "cleanrooms:GetIdMappingTable",
        "cleanrooms:GetIdNamespaceAssociation",
```

```
        "cleanrooms:GetMembership",
        "cleanrooms:GetPrivacyBudgetTemplate",
        "cleanrooms:GetProtectedQuery",
        "cleanrooms:GetSchema",
        "cleanrooms:GetSchemaAnalysisRule",
        "cleanrooms:ListAnalysisTemplates",
        "cleanrooms:ListCollaborationAnalysisTemplates",
        "cleanrooms:ListCollaborationConfiguredAudienceModelAssociations",
        "cleanrooms:ListCollaborationIdNamespaceAssociations",
        "cleanrooms:ListCollaborationPrivacyBudgetTemplates",
        "cleanrooms:ListCollaborationPrivacyBudgets",
        "cleanrooms:ListCollaborations",
        "cleanrooms:ListConfiguredAudienceModelAssociations",
        "cleanrooms:ListConfiguredTableAssociations",
        "cleanrooms:ListConfiguredTables",
        "cleanrooms:ListIdMappingTables",
        "cleanrooms:ListIdNamespaceAssociations",
        "cleanrooms:ListMembers",
        "cleanrooms:ListMemberships",
        "cleanrooms:ListPrivacyBudgetTemplates",
        "cleanrooms:ListPrivacyBudgets",
        "cleanrooms:ListProtectedQueries",
        "cleanrooms:ListSchemas",
        "cleanrooms:ListTagsForResource",
        "cleanrooms:PreviewPrivacyImpact",
        "cloud9:Describe*",
        "cloud9:ListEnvironments",
        "clouddirectory:ListDirectories",
        "cloudformation:DescribeStack*",
        "cloudformation:GetStackPolicy",
        "cloudformation:GetTemplate",
        "cloudformation:ListStack*",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomainEndpointOptions",
        "cloudsearch:DescribeDomains",
        "cloudsearch:DescribeServiceAccessPolicies",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetEventSelectors",
        "cloudtrail:GetInsightSelectors",
        "cloudtrail:GetTrail",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListTags",
        "cloudtrail:ListTrails",
```

```
        "cloudtrail:LookupEvents",
        "cloudwatch:Describe*",
        "cloudwatch:GetDashboard",
        "cloudwatch:ListDashboards",
        "cloudwatch:ListTagsForResource",
        "codeartifact:GetDomainPermissionsPolicy",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "codeartifact:ListRepositories",
        "codebuild:BatchGetProjects",
        "codebuild:GetResourcePolicy",
        "codebuild:ListProjects",
        "codebuild:ListSourceCredentials",
        "codecommit:BatchGetRepositories",
        "codecommit:GetBranch",
        "codecommit:GetObjectIdentifier",
        "codecommit:GetRepository",
        "codecommit:GetRepositoryTriggers",
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:GetJobDetails",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelines",
        "codestar:Describe*",
        "codestar:List*",
        "cognito-identity:Describe*",
        "cognito-identity:GetIdentityPoolRoles",
        "cognito-identity:ListIdentityPools",
        "cognito-identity:ListTagsForResource",
        "cognito-idp:Describe*",
        "cognito-idp:ListDevices",
        "cognito-idp:ListGroups",
        "cognito-idp:ListIdentityProviders",
        "cognito-idp:ListResourceServers",
        "cognito-idp:ListTagsForResource",
        "cognito-idp:ListUserImportJobs",
        "cognito-idp:ListUserPoolClients",
        "cognito-idp:ListUserPools",
        "cognito-idp:ListUsers",
        "cognito-idp:ListUsersInGroup",
        "cognito-sync:Describe*",
```

```
        "cognito-sync:List*",
        "comprehend:Describe*",
        "comprehend:List*",
        "comprehendmedical:ListICD10CMInferenceJobs",
        "comprehendmedical:ListPHIDetectionJobs",
        "comprehendmedical:ListRxNormInferenceJobs",
        "comprehendmedical:ListSNOMEDCTInferenceJobs",
        "config:BatchGetAggregateResourceConfig",
        "config:BatchGetResourceConfig",
        "config:Deliver*",
        "config:Describe*",
        "config:Get*",
        "config:List*",
        "config:SelectAggregateResourceConfig",
        "config:SelectResourceConfig",
        "connect:ListApprovedOrigins",
        "connect:ListInstanceAttributes",
        "connect:ListInstances",
        "connect:ListInstanceStorageConfigs",
        "connect:ListIntegrationAssociations",
        "connect:ListLambdaFunctions",
        "connect:ListLexBots",
        "connect:ListSecurityKeys",
        "databrew:DescribeDataset",
        "databrew:DescribeProject",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "dataexchange:ListDataSets",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:EvaluateExpression",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ValidatePipelineDefinition",
        "datasync:Describe*",
        "datasync:List*",
        "dax:Describe*",
        "dax:ListTags",
        "deepracer:ListModels",
        "detective:GetGraphIngestState",
        "detective:ListGraphs",
        "detective:ListMembers",
        "devicefarm:ListProjects",
```

```
        "directconnect:Describe*",
        "discovery:DescribeAgents",
        "discovery:DescribeConfigurations",
        "discovery:DescribeContinuousExports",
        "discovery:DescribeExportConfigurations",
        "discovery:DescribeExportTasks",
        "discovery:DescribeImportTasks",
        "dms:Describe*",
        "dms:ListTagsForResource",
        "docdb-elastic:ListClusters",
        "ds:DescribeDirectories",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeExport",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeKinesisStreamingDestination",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:Describe*",
        "ec2:GetAllowedImagesSettings",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:GetImageBlockPublicAccessState",
        "ec2:GetInstanceMetadataDefaults",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:GetNetworkInsightsAccessScopeAnalysisFindings",
        "ec2:GetNetworkInsightsAccessScopeContent",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:GetSnapshotBlockPublicAccessState",
        "ec2:GetTransitGatewayAttachmentPropagations",
        "ec2:GetTransitGatewayMulticastDomainAssociations",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayPrefixListReferences",
        "ec2:GetTransitGatewayRouteTableAssociations",
        "ec2:GetTransitGatewayRouteTablePropagations",
        "ec2:SearchTransitGatewayRoutes",
        "ec2:SearchTransitGatewayRoutes",
        "ecr-public:DescribeImages",
```

```
        "ecr-public:DescribeImageTags",
        "ecr-public:DescribeRegistries",
        "ecr-public:DescribeRepositories",
        "ecr-public:GetRegistryCatalogData",
        "ecr-public:GetRepositoryCatalogData",
        "ecr-public:GetRepositoryPolicy",
        "ecr-public:ListTagsForResource",
        "ecr:BatchGetRepositoryScanningConfiguration",
        "ecr:DescribeImages",
        "ecr:DescribeImageScanFindings",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:GetLifecyclePolicy",
        "ecr:GetRegistryPolicy",
        "ecr:GetRegistryScanningConfiguration",
        "ecr:GetRepositoryPolicy",
        "ecr:ListImages",
        "ecr:ListTagsForResource",
        "ecs:Describe*",
        "ecs:List*",
        "eks:DescribeCluster",
        "eks:DescribeFargateProfile",
        "eks:DescribeNodeGroup",
        "eks:ListClusters",
        "eks:ListFargateProfiles",
        "eks:ListNodeGroups",
        "eks:ListTagsForResource",
        "eks:ListUpdates",
        "elasticache:Describe*",
        "elasticache:ListTagsForResource",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:ListTagsForResource",
        "elasticfilesystem:DescribeAccessPoints",
        "elasticfilesystem:DescribeAccountPreferences",
        "elasticfilesystem:DescribeBackupPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "elasticfilesystem:DescribeFileSystems",
        "elasticfilesystem:DescribeLifecycleConfiguration",
        "elasticfilesystem:DescribeMountTargets",
        "elasticfilesystem:DescribeMountTargetSecurityGroups",
        "elasticfilesystem:DescribeReplicationConfigurations",
        "elasticfilesystem:DescribeTags",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
```

```
        "elasticmapreduce:GetAutoTerminationPolicy",
        "elasticmapreduce:GetBlockPublicAccessConfiguration",
        "elasticmapreduce:GetManagedScalingPolicy",
        "elasticmapreduce:ListClusters",
        "elasticmapreduce:ListInstances",
        "elasticmapreduce:ListSecurityConfigurations",
        "elastictranscoder:ListPipelines",
        "emr-serverless:GetApplication",
        "emr-serverless:ListApplications",
        "emr-serverless:ListJobRuns",
        "entityresolution:GetIdNamespace",
        "es:Describe*",
        "es:GetCompatibleVersions",
        "es:ListDomainNames",
        "es:ListElasticsearchInstanceTypeDetails",
        "es:ListElasticsearchVersions",
        "es:ListTags",
        "events:Describe*",
        "events:List*",
        "events:TestEventPattern",
        "finspace:ListEnvironments",
        "finspace:ListKxEnvironments",
        "firehose:Describe*",
        "firehose:List*",
        "fms:ListComplianceStatus",
        "fms:ListPolicies",
        "forecast:ListDatasets",
        "frauddetector:GetDetectors",
        "fsx:Describe*",
        "fsx:List*",
        "gamelift:ListBuilds",
        "gamelift:ListFleets",
        "geo:ListMaps",
        "glacier:DescribeVault",
        "glacier:GetDataRetrievalPolicy",
        "glacier:GetVaultAccessPolicy",
        "glacier:GetVaultLock",
        "glacier:ListVaults",
        "globalaccelerator:Describe*",
        "globalaccelerator:List*",
        "glue:GetCrawlers",
        "glue:GetDatabases",
        "glue:GetDataCatalogEncryptionSettings",
        "glue:GetDevEndpoints",
```

```
        "glue:GetJobs",
        "glue:GetResourcePolicy",
        "glue:GetSecurityConfiguration",
        "glue:GetSecurityConfigurations",
        "glue:GetTags",
        "grafana:ListWorkspaces",
        "greengrass:List*",
        "guardduty:DescribePublishingDestination",
        "guardduty:DescribeOrganizationConfiguration",
        "guardduty:DescribeMalwareScans",
        "guardduty:Get*",
        "guardduty:List*",
        "health:DescribeAffectedAccountsForOrganization",
        "health:DescribeAffectedEntities",
        "health:DescribeAffectedEntitiesForOrganization",
        "health:DescribeEntityAggregates",
        "health:DescribeEventAggregates",
        "health:DescribeEventDetails",
        "health:DescribeEventDetailsForOrganization",
        "health:DescribeEvents",
        "health:DescribeEventsForOrganization",
        "health:DescribeEventTypes",
        "health:DescribeHealthServiceStatusForOrganization",
        "healthlake:ListFHIRDatastores",
        "honeycode:ListTables",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy",
        "identitystore:DescribeGroupMembership",
        "identitystore:GetGroupId",
        "identitystore:GetGroupMembershipId",
        "identitystore:GetUserId",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:ListGroupMembershipsForMember",
        "identitystore:ListGroups",
        "identitystore:ListUsers",
        "inspector:Describe*",
        "inspector:Get*",
        "inspector:List*",
        "inspector:Preview*",
```

```
        "inspector2:BatchGetAccountStatus",
        "inspector2:BatchGetFreeTrialInfo",
        "inspector2:DescribeOrganizationConfiguration",
        "inspector2:GetConfiguration",
        "inspector2:GetDelegatedAdminAccount",
        "inspector2:GetFindingsReportStatus",
        "inspector2:GetMember",
        "inspector2:ListAccountPermissions",
        "inspector2:ListCoverage",
        "inspector2:ListCoverageStatistics",
        "inspector2:ListDelegatedAdminAccounts",
        "inspector2:ListFilters",
        "inspector2:ListFindingAggregations",
        "inspector2:ListFindings",
        "inspector2:ListTagsForResource",
        "inspector2:ListUsageTotals",
        "iot:Describe*",
        "iot:GetPolicy",
        "iot:GetPolicyVersion",
        "iot:List*",
        "iotanalytics:ListChannels",
        "iotevents:ListInputs",
        "iotfleetwise:ListModelManifests",
        "iotsitewise:DescribeGatewayCapabilityConfiguration",
        "iotsitewise:ListAssetModels",
        "iotsitewise:ListGateways",
        "iottwinmaker:ListWorkspaces",
        "kafka-cluster:Describe*",
        "kafka:Describe*",
        "kafka:GetBootstrapBrokers",
        "kafka:GetCompatibleKafkaVersions",
        "kafka:List*",
        "kafkaconnect:Describe*",
        "kafkaconnect:List*",
        "kendra:DescribeIndex",
        "kendra:ListDataSources",
        "kendra:ListIndices",
        "kendra:ListTagsForResource",
        "kinesis:DescribeLimits",
        "kinesis:DescribeStream",
        "kinesis:DescribeStreamConsumer",
        "kinesis:DescribeStreamSummary",
        "kinesis:ListShards",
        "kinesis:ListStreamConsumers",
```

```
        "kinesis:ListStreams",
        "kinesis:ListTagsForStream",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kinesisvideo:DescribeEdgeConfiguration",
        "kinesisvideo:DescribeMappedResourceConfiguration",
        "kinesisvideo:DescribeMediaStorageConfiguration",
        "kinesisvideo:DescribeNotificationConfiguration",
        "kinesisvideo:DescribeSignalingChannel",
        "kinesisvideo:DescribeStream",
        "kinesisvideo:ListSignalingChannels",
        "kinesisvideo:ListStreams",
        "kinesisvideo:ListTagsForResource",
        "kinesisvideo:ListTagsForStream",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:GetAccountSettings",
        "lambda:GetFunctionConfiguration",
        "lambda:GetFunctionEventInvokeConfig",
        "lambda:GetLayerVersionPolicy",
        "lambda:GetPolicy",
        "lambda:List*",
        "lex:DescribeBot",
        "lex:DescribeResourcePolicy",
        "lex:ListBots",
        "license-manager:List*",
        "lightsail:GetBuckets",
        "lightsail:GetContainerServices",
        "lightsail:GetDisks",
        "lightsail:GetDiskSnapshots",
        "lightsail:GetInstances",
        "lightsail:GetLoadBalancers",
        "logs:Describe*",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:ListTagsForResource",
        "logs:ListTagsLogGroup",
        "lookoutequipment:ListDatasets",
        "lookoutmetrics:ListAnomalyDetectors",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
```

```
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:DescribeMLModels",
        "macie2:ListFindings",
        "managedblockchain:ListNetworks",
        "mechanicalturk:ListHITs",
        "mediaconnect:Describe*",
        "mediaconnect:List*",
        "medialive:ListChannels",
        "mediapackage-vod:DescribePackagingGroup",
        "mediapackage-vod:ListPackagingGroups",
        "mediapackage:DescribeOriginEndpoint",
        "mediapackage:ListOriginEndpoints",
        "mediastore:GetContainerPolicy",
        "mediastore:GetCorsPolicy",
        "mediastore:ListContainers",
        "memorydb:DescribeClusters",
        "mq:DescribeBroker",
        "mq:DescribeBrokerEngineTypes",
        "mq:DescribeBrokerInstanceOptions",
        "mq:DescribeConfiguration",
        "mq:DescribeConfigurationRevision",
        "mq:DescribeUser",
        "mq:ListBrokers",
        "mq:ListConfigurationRevisions",
        "mq:ListConfigurations",
        "mq:ListTags",
        "mq:ListUsers",
        "network-firewall:DescribeFirewall",
        "network-firewall:DescribeFirewallPolicy",
        "network-firewall:DescribeLoggingConfiguration",
        "network-firewall:DescribeResourcePolicy",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:ListFirewallPolicies",
        "network-firewall:ListFirewalls",
        "network-firewall:ListRuleGroups",
        "networkmanager:DescribeGlobalNetworks",
        "nimble:ListStudios",
        "opsworks-cm:DescribeServers",
        "opsworks:DescribeStacks",
        "organizations:Describe*",
        "organizations:List*",
        "pcs:GetCluster",
        "pcs:GetComputeNodeGroup",
```

```
        "pcs:GetQueue",
        "pcs:ListClusters",
        "pcs:ListComputeNodeGroups",
        "pcs:ListQueues",
        "pcs:ListTagsForResource",
        "personalize:DescribeDatasetGroup",
        "personalize:ListDatasetGroups",
        "private-networks:ListNetworks",
        "profile:GetDomain",
        "profile:ListDomains",
        "profile:ListIntegrations",
        "qbusiness:ListApplications",
        "qbusiness:ListDataSources",
        "qbusiness:ListDataSourceSyncJobs",
        "qbusiness:ListDocuments",
        "qbusiness:ListGroups",
        "qbusiness:ListIndices",
        "qbusiness:ListPlugins",
        "qbusiness:ListRetrievers",
        "qbusiness:ListSubscriptions",
        "qbusiness:ListTagsForResource",
        "qbusiness:ListWebExperiences",
        "qldb:DescribeJournalS3Export",
        "qldb:DescribeLedger",
        "qldb:ListJournalS3Exports",
        "qldb:ListJournalS3ExportsForLedger",
        "qldb:ListLedgers",
        "quicksight:Describe*",
        "quicksight:List*",
        "ram:GetResourceShares",
        "ram:List*",
        "rds:Describe*",
        "rds:DownloadDBLogFilePortion",
        "rds:ListTagsForResource",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:ListTagsForResource",
        "redshift-serverless:ListWorkgroups",
        "redshift:Describe*",
        "rekognition:Describe*",
        "rekognition:List*",
        "resource-groups:ListGroupResources",
        "robomaker:Describe*",
        "robomaker:List*",
        "rolesanywhere:GetCrl",
```

```
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:ListDomains",
        "route53domains:ListOperations",
        "route53domains:ListTagsForDomain",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3-outposts:ListEndpoints",
        "s3-outposts:ListOutpostsWithS3",
        "s3-outposts:ListSharedEndpoints",
        "s3:DescribeJob",
        "s3:GetAccelerateConfiguration",
        "s3:GetAccessGrantsInstanceResourcePolicy",
        "s3:GetAccessPoint",
        "s3:GetAccessPointConfigurationForObjectLambda",
        "s3:GetAccessPointPolicy",
        "s3:GetAccessPointPolicyForObjectLambda",
        "s3:GetAccessPointPolicyStatus",
        "s3:GetAccessPointPolicyStatusForObjectLambda",
        "s3:GetAccessPointForObjectLambda",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetAnalyticsConfiguration",
        "s3:GetBucket*",
        "s3:GetEncryptionConfiguration",
        "s3:GetInventoryConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetMetricsConfiguration",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetReplicationConfiguration",
```

```
        "s3:GetStorageLensGroup",
        "s3:GetStorageLensConfiguration",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "s3:ListAccessPointsForObjectLambda",
        "s3:ListStorageLensGroups",
        "s3:ListJobs",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances",
        "s3:ListAccessGrants",
        "s3:ListStorageLensConfigurations",
        "s3express:ListAllMyDirectoryBuckets",
        "s3express:GetEncryptionConfiguration",
        "s3express:GetBucketPolicy",
        "s3-object-lambda:GetObjectAcl",
        "s3-object-lambda:GetObjectVersionAcl",
        "s3tables:ListTableBuckets",
        "s3tables:ListNamespaces",
        "s3tables:ListTables",
        "s3tables:GetNamespace",
        "s3tables:GetTableBucketPolicy",
        "s3tables:GetTableBucketMaintenanceConfiguration",
        "s3tables:GetTableMaintenanceConfiguration",
        "s3tables:GetTablePolicy",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "schemas:DescribeCodeBinding",
        "schemas:DescribeDiscoverer",
        "schemas:DescribeRegistry",
        "schemas:DescribeSchema",
        "schemas:GetResourcePolicy",
        "schemas:ListDiscoverers",
        "schemas:ListRegistries",
        "schemas:ListSchemas",
        "schemas:ListSchemaVersions",
        "schemas:ListTagsForResource",
        "sdb:DomainMetadata",
        "sdb:ListDomains",
        "secretsmanager:DescribeSecret",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:ListSecrets",
        "secretsmanager:ListSecretVersionIds",
```

```
        "securityhub:BatchGetAutomationRules",
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:BatchGetControlEvaluations",
        "securityhub:BatchGetSecurityControls",
        "securityhub:BatchGetStandardsControlAssociations",
        "securityhub:Describe*",
        "securityhub:Get*",
        "securityhub:List*",
        "serverlessrepo:GetApplicationPolicy",
        "serverlessrepo:List*",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServices",
        "servicequotas:ListTagsForResource",
        "ses:Describe*",
        "ses:GetAccount",
        "ses:GetAccountSendingEnabled",
        "ses:GetConfigurationSet",
        "ses:GetConfigurationSetEventDestinations",
        "ses:GetDedicatedIps",
        "ses:GetEmailIdentity",
        "ses:GetIdentityDkimAttributes",
        "ses:GetIdentityPolicies",
        "ses:GetIdentityVerificationAttributes",
        "ses:ListConfigurationSets",
        "ses:ListDedicatedIpPools",
        "ses:ListIdentities",
        "ses:ListIdentityPolicies",
        "ses:ListReceiptFilters",
        "ses:ListReceiptRuleSets",
        "ses:ListVerifiedEmailAddresses",
        "shield:Describe*",
        "shield:GetSubscriptionState",
        "shield:List*",
        "snowball:ListClusters",
        "snowball:ListJobs",
```

```
        "sns:GetPlatformApplicationAttributes",
        "sns:GetTopicAttributes",
        "sns:ListSubscriptions",
        "sns:ListSubscriptionsByTopic",
        "sns:ListTagsForResource",
        "sns:ListTopics",
        "sqs:GetQueueAttributes",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:Describe*",
        "ssm:GetAutomationExecution",
        "ssm:GetServiceSetting",
        "ssm:ListAssociations",
        "ssm:ListAssociationVersions",
        "ssm:ListCommands",
        "ssm:ListComplianceItems",
        "ssm:ListComplianceSummaries",
        "ssm:ListDocumentMetadataHistory",
        "ssm:ListDocuments",
        "ssm:ListDocumentVersions",
        "ssm:ListInventoryEntries",
        "ssm:ListOpsMetadata",
        "ssm:ListResourceComplianceSummaries",
        "ssm:ListResourceDataSync",
        "ssm:ListTagsForResource",
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribePermissionSet",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribeApplication",
        "sso:DescribeApplicationAssignment",
        "sso:DescribeApplicationProvider",
        "sso:DescribeInstance",
        "sso:DescribeInstanceAccessControlAttributeConfiguration",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeTrustedTokenIssuer",
        "sso:GetApplicationAccessScope",
        "sso:GetApplicationAssignmentConfiguration",
        "sso:GetApplicationAuthenticationMethod",
        "sso:GetApplicationGrant",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetPermissionsBoundaryForPermissionSet",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
```

```
        "sso:ListAccountAssignments",
        "sso:ListAccountAssignmentsForPrincipal",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationAccessScopes",
        "sso:ListApplicationAssignments",
        "sso:ListApplicationAssignmentsForPrincipal",
        "sso:ListApplicationAuthenticationMethods",
        "sso:ListApplicationGrants",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplicationProviders",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListCustomerManagedPolicyReferencesInPermissionSet",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
        "sso:ListProfiles",
        "sso:ListTagsForResource",
        "sso:ListTrustedTokenIssuers",
        "states:DescribeStateMachine",
        "states:ListStateMachines",
        "storagegateway:DescribeBandwidthRateLimit",
        "storagegateway:DescribeCache",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:DescribeMaintenanceStartTime",
        "storagegateway:DescribeNFSFileShares",
        "storagegateway:DescribeSnapshotSchedule",
        "storagegateway:DescribeStorediSCSIVolumes",
        "storagegateway:DescribeTapeArchives",
        "storagegateway:DescribeTapeRecoveryPoints",
        "storagegateway:DescribeTapes",
        "storagegateway:DescribeUploadBuffer",
        "storagegateway:DescribeVTLDevices",
        "storagegateway:DescribeWorkingStorage",
        "storagegateway:List*",
        "sts:GetAccessKeyInfo",
        "support:DescribeTrustedAdvisorCheckRefreshStatuses",
        "support:DescribeTrustedAdvisorCheckResult",
```

```
        "support:DescribeTrustedAdvisorChecks",
        "support:DescribeTrustedAdvisorCheckSummaries",
        "synthetics:DescribeCanaries",
        "synthetics:DescribeCanariesLastRun",
        "synthetics:DescribeRuntimeVersions",
        "synthetics:GetCanary",
        "synthetics:GetCanaryRuns",
        "synthetics:GetGroup",
        "synthetics:ListAssociatedGroups",
        "synthetics:ListGroupResources",
        "synthetics:ListGroups",
        "synthetics:ListTagsForResource",
        "tag:GetResources",
        "tag:GetTagKeys",
        "transcribe:GetCallAnalyticsCategory",
        "transcribe:GetMedicalVocabulary",
        "transcribe:GetVocabulary",
        "transcribe:GetVocabularyFilter",
        "transcribe:ListCallAnalyticsCategories",
        "transcribe:ListCallAnalyticsJobs",
        "transcribe:ListLanguageModels",
        "transcribe:ListMedicalTranscriptionJobs",
        "transcribe:ListMedicalVocabularies",
        "transcribe:ListTagsForResource",
        "transcribe:ListTranscriptionJobs",
        "transcribe:ListVocabularies",
        "transcribe:ListVocabularyFilters",
        "transfer:Describe*",
        "transfer:List*",
        "translate:List*",
        "trustedadvisor:Describe*",
        "voiceid:DescribeDomain",
        "waf-regional:GetWebACL",
        "waf-regional:ListResourcesForWebACL",
        "waf-regional:ListTagsForResource",
        "waf-regional:ListWebACLs",
        "waf:GetWebACL",
        "waf:ListTagsForResource",
        "waf:ListWebACLs",
        "wafv2:GetLoggingConfiguration",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:ListIPSets",
```

```
        "wafv2:ListLoggingConfigurations",
        "wafv2:ListRegexPatternSets",
        "wafv2:ListResourcesForWebACL",
        "wafv2:ListRuleGroups",
        "wafv2:ListTagsForResource",
        "wafv2:ListWebACLs",
        "wisdom:GetAssistant",
        "workdocs:DescribeResourcePermissions",
        "workspaces:Describe*",
        "xray:GetEncryptionConfig",
        "xray:GetGroup",
        "xray:GetGroups",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetTraceSummaries",
        "xray:ListTagsForResource"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "APIGatewayAccess",
      "Effect" : "Allow",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
```

```
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityLakeResourceManagementServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf die Verwaltung von Ressourcen, die von Security Lake erstellt wurden.

`SecurityLakeResourceManagementServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 14. November 2024, 22:10 UTC
- Bearbeitete Zeit: 19. November 2025, 18:49 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeResourceManagementServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "ReadEventBridgeRules",
      "Effect" : "Allow",
      "Action" : [
        "events:ListRules"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeEventRules",
      "Effect" : "Allow",
      "Action" : [
        "events:PutRule"
      ],
      "Resource" : "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeLambdaConfigurations",
      "Effect" : "Allow",
      "Action" : [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
```

```
    },
    {
      "Sid" : "DeletePartitionUpdaterLambda",
      "Effect" : "Allow",
      "Action" : "lambda:DeleteFunction",
      "Resource" :
"arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowListLambdaEventSourceMappings",
      "Effect" : "Allow",
      "Action" : [
        "lambda:ListEventSourceMappings"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowUpdateLambdaEventSourceMapping",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        },
        "ArnLike" : {
          "lambda:FunctionArn" :
"arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
```

```
      "Sid" : "AllowUpdateLambdaConfigs",
      "Effect" : "Allow",
      "Action" : [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource" : "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-
*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeGlueResources",
      "Effect" : "Allow",
      "Action" : [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource" : [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeConfigurationManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
```

```
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowMetaDataCompactionAndManagement",
      "Effect" : "Allow",
      "Action" : [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource" : [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ReadSecurityLakeLambdaLogs",
      "Effect" : "Allow",
      "Action" : [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource" : [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "ManageSecurityLakeSQSQueue",
      "Effect" : "Allow",
      "Action" : [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource" : [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "AllowDataLakeManagement",
      "Effect" : "Allow",
      "Action" : [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
```

```
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SecurityLakeServiceLinkedRole

Beschreibung: Diese Richtlinie gewährt die Erlaubnis, den Amazon Security Lake-Service in Ihrem Namen zu betreiben

`SecurityLakeServiceLinkedRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 29. November 2022, 14:03 UTC
- Bearbeitete Zeit: 19. April 2024, 16:00 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SecurityLakeServiceLinkedRole`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "OrganizationsPolicies",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization"
      ],
      "Resource" : [
        "*"
      ]
    },
    {
      "Sid" : "DescribeOrgAccounts",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : [
        "arn:aws:organizations::*:account/o-*/*"
      ]
    },
    {
      "Sid" : "AllowManagementOfServiceLinkedChannel",
      "Effect" : "Allow",
      "Action" : [
        "cloudtrail:CreateServiceLinkedChannel",
        "cloudtrail:DeleteServiceLinkedChannel",
        "cloudtrail:GetServiceLinkedChannel",
        "cloudtrail:UpdateServiceLinkedChannel"
      ],
      "Resource" : "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-lake/*"
    },
    {
      "Sid" : "AllowListServiceLinkedChannel",
      "Effect" : "Allow",
```

```
      "Action" : [
        "cloudtrail:ListServiceLinkedChannels"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "DescribeAnyVpc",
      "Effect" : "Allow",
      "Action" : [
        "ec2:DescribeVpcs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "ListDelegatedAdmins",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "organizations:ServicePrincipal" : "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AllowWafLoggingConfiguration",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration",
        "wafv2:GetLoggingConfiguration",
        "wafv2:ListLoggingConfigurations",
        "wafv2:DeleteLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "wafv2:LogScope" : "SecurityLake"
        }
      }
    },
    {
      "Sid" : "AllowPutLoggingConfiguration",
```

```
      "Effect" : "Allow",
      "Action" : [
        "wafv2:PutLoggingConfiguration"
      ],
      "Resource" : "*",
      "Condition" : {
        "ArnLike" : {
          "wafv2:LogDestinationResource" : "arn:aws:s3:::aws-waf-logs-security-lake-*"
        }
      }
    },
    {
      "Sid" : "ListWebACLs",
      "Effect" : "Allow",
      "Action" : [
        "wafv2:ListWebACLs"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "LogDelivery",
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "wafv2.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigration_ServiceRole

Beschreibung: Berechtigungen für die Migration des AWS Servermigrationsdienstes VMs nach EC2: Ermöglicht dem Servermigrationsdienst, die migrierten Ressourcen dem EC2 Konto des Kunden zuzuweisen.

`ServerMigration_ServiceRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServerMigration_ServiceRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 11. August 2020, 20:41 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:26 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigration_ServiceRole`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*",
      "Condition" : {
        "Null" : {
          "cloudformation:ResourceTypes" : "false"
        },
        "ForAllValues:StringEquals" : {
          "cloudformation:ResourceTypes" : [
            "AWS::EC2::Instance",
            "AWS::ApplicationInsights::Application",
            "AWS::ResourceGroups::Group"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStack",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources",
        "cloudformation:GetTemplate"
      ],
      "Resource" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:ValidateTemplate",
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:CreateBucket",
```

```
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource" : "arn:aws:s3:::sms-app-*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:CreateReplicationJob",
        "sms:DeleteReplicationJob",
        "sms:GetReplicationJobs",
        "sms:GetReplicationRuns",
        "sms:GetServers",
        "sms:ImportServerCatalog",
        "sms:StartOnDemandReplicationRun",
        "sms:UpdateReplicationJob"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : [
        "arn:aws:ssm:*::document/AWS-RunRemoteScript",
        "arn:aws:s3:::sms-app-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "ssm:SendCommand",
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringEquals" : {
          "ssm:resourceTag/UseForSMSApplicationValidation" : [
            "true"
          ]
        }
```

```
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringEquals" : {
          "ec2:CreateAction" : "CopySnapshot"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CopySnapshot",
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "aws:RequestTag/SMSJobId" : [
            "sms-*"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:DeleteSnapshot"
      ],
      "Resource" : "arn:aws:ec2:*:*:snapshot/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/SMSJobId" : [
            "sms-*"
          ]
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CopyImage",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSnapshotAttribute",
        "ec2:DeregisterImage",
        "ec2:ImportImage",
        "ec2:DescribeImportImageTasks",
        "ec2:GetEbsEncryptionByDefault"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:GetRole",
        "iam:GetInstanceProfile"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
```

```
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEqualsIfExists" : {
          "iam:PassedToService" : "cloudformation.amazonaws.com"
        },
        "StringLike" : {
          "iam:AssociatedResourceArn" : "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationConnector

Beschreibung: Berechtigungen, zu denen der AWS Server Migration Connector VMs migrieren kann EC2. Ermöglicht die Kommunikation mit dem AWS Server Migration Service, den read/write Zugriff auf S3-Buckets, die mit 'sms-b-' und 'import-to-ec2' beginnen, sowie auf die Buckets, die für das AWS Server Migration Connector-Upgrade, die Server Migration Connector-Registrierung bei AWS und das AWS Hochladen von Metriken verwendet werden. AWS

`ServerMigrationConnector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `ServerMigrationConnector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Oktober 2016, 21:45 Uhr UTC
- Bearbeitete Zeit: 24. Oktober 2016, 21:45 UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationConnector`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "iam:GetUser",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "sms:SendMessage",
        "sms:GetMessages"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
```

```
      "Action" : [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutLifecycleConfiguration",
        "s3:AbortMultipartUpload",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts"
      ],
      "Resource" : [
        "arn:aws:s3:::sms-b-*",
        "arn:aws:s3:::import-to-ec2-*",
        "arn:aws:s3:::server-migration-service-upgrade",
        "arn:aws:s3:::server-migration-service-upgrade/*",
        "arn:aws:s3:::connector-platform-upgrade-info/*",
        "arn:aws:s3:::connector-platform-upgrade-info",
        "arn:aws:s3:::connector-platform-upgrade-bundles/*",
        "arn:aws:s3:::connector-platform-upgrade-bundles",
        "arn:aws:s3:::connector-platform-release-notes/*",
        "arn:aws:s3:::connector-platform-release-notes"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : "awsconnector:*",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "SNS:Publish"
      ],
      "Resource" : "arn:aws:sns:*:*:metrics-sns-topic-for-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceConsoleFullAccess

Beschreibung: Erforderliche Berechtigungen zur Nutzung aller Funktionen der Server Migration Service Console

`ServerMigrationServiceConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServerMigrationServiceConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 09. Mai 2020, 17:18 Uhr UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:00 Uhr UTC
- ARN: `arn:aws:iam::aws:policy/ServerMigrationServiceConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "sms:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "cloudformation:ListStacks",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : "s3:ListAllMyBuckets",
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Action" : [
        "ec2:DescribeKeyPairs",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
```

```
        "iam:ListRoles"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "sms.amazonaws.com"
        }
      },
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:GetInstanceProfile",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceLaunchRole

Beschreibung: Berechtigungen, die es dem AWS Server Migration Service ermöglichen, für den Start migrierter Server und Anwendungen relevante AWS Ressourcen AWS-Konto für den Kunden zu erstellen und zu aktualisieren.

`ServerMigrationServiceLaunchRole`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServerMigrationServiceLaunchRole` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 26. November 2018, 19:53 UTC
- Bearbeitete Zeit: 15. Oktober 2020, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceLaunchRole`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifyInstanceAttribute",
        "ec2:StopInstances",
        "ec2:StartInstances",
        "ec2:TerminateInstances"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
```

```
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "ec2:CreateTags",
      "Resource" : "arn:aws:ec2:*:*:instance/*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:DisassociateIamInstanceProfile",
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource" : "arn:aws:ec2:*:*:instance/*",
      "Condition" : {
        "StringLike" : {
          "ec2:ResourceTag/aws:cloudformation:stack-id" :
"arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:PassedToService" : "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:RunInstances",
        "ec2:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
```

```
        "applicationinsights:Describe*",
        "applicationinsights:List*",
        "cloudformation:ListStackResources",
        "cloudformation:DescribeStacks"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "applicationinsights:CreateApplication",
        "applicationinsights:CreateComponent",
        "applicationinsights:UpdateApplication",
        "applicationinsights:DeleteApplication",
        "applicationinsights:UpdateComponentConfiguration",
        "applicationinsights:DeleteComponent"
      ],
      "Resource" : "arn:aws:applicationinsights:*:*:application/resource-group/sms-app-
*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:UpdateGroup",
        "resource-groups:DeleteGroup"
      ],
      "Resource" : "arn:aws:resource-groups:*:*:group/sms-app-*",
      "Condition" : {
        "StringLike" : {
          "aws:ResourceTag/aws:cloudformation:stack-id" :
 "arn:aws:cloudformation:*:*:stack/sms-app-*/*"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : [
        "arn:aws:iam::*:role/aws-service-role/application-insights.amazonaws.com/
AWSServiceRoleForApplicationInsights"
```

```
      ],
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "application-insights.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServerMigrationServiceRoleForInstanceValidation

Beschreibung: Berechtigungen, die es der AWS SMS ermöglichen, das verwendete Datenüberprüfungsskript auszuführen und das Skript success/failure zurück an SMS zu senden

`ServerMigrationServiceRoleForInstanceValidation`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServerMigrationServiceRoleForInstanceValidation` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 20. Juli 2020, 22:25 Uhr UTC
- Bearbeitete Zeit: 20. Juli 2020, 22:25 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/ServerMigrationServiceRoleForInstanceValidation`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "s3:GetObject",
      "Resource" : "arn:aws:s3:::sms-app-*/*"
    },
    {
      "Effect" : "Allow",
      "Action" : "sms:NotifyAppValidationOutput",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasFullAccess

Beschreibung: Bietet vollen Zugriff auf Service Quotas

`ServiceQuotasFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServiceQuotasFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2019, 15:44 Uhr UTC
- Bearbeitete Zeit: 4. Februar 2021, 21:29 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasFullAccess`

Version der Richtlinie

Richtlinienversion: v4 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:PutMetricAlarm",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
```

```
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "cloudwatch:DeleteAlarms"
      ],
      "Resource" : "*",
      "Condition" : {
        "Null" : {
          "aws:ResourceTag/ServiceQuotaMonitor" : "false"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringLike" : {
          "organizations:ServicePrincipal" : [
            "servicequotas.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource" : "*",
```

```
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : "servicequotas.amazonaws.com"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Service Quotas

`ServiceQuotasReadOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ServiceQuotasReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 24. Juni 2019, 15:31 UTC
- Bearbeitete Zeit: 13. Oktober 2025, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/ServiceQuotasReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "autoscaling:DescribeAccountLimits",
        "cloudformation:DescribeAccountLimits",
        "cloudwatch:DescribeAlarmsForMetric",
        "cloudwatch:DescribeAlarms",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "dynamodb:DescribeLimits",
        "elasticloadbalancing:DescribeAccountLimits",
        "iam:GetAccountSummary",
        "kinesis:DescribeLimits",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "rds:DescribeAccountAttributes",
        "route53:GetAccountLimit",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "servicequotas:GetAssociationForServiceQuotaTemplate",
        "servicequotas:GetAWSDefaultServiceQuota",
        "servicequotas:GetRequestedServiceQuotaChange",
        "servicequotas:GetServiceQuota",
        "servicequotas:GetServiceQuotaIncreaseRequestFromTemplate",
        "servicequotas:ListAWSDefaultServiceQuotas",
        "servicequotas:ListRequestedServiceQuotaChangeHistory",
        "servicequotas:ListRequestedServiceQuotaChangeHistoryByQuota",
        "servicequotas:ListServices",
        "servicequotas:ListServiceQuotas",
        "servicequotas:ListServiceQuotaIncreaseRequestsInTemplate",
        "servicequotas:ListTagsForResource",
        "servicequotas:GetAutoManagementConfiguration",
```

```
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:GetNotificationConfiguration",
        "notifications:GetEventRule",
        "notifications:ListNotificationHubs",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:GetEmailContact",
        "chatbot:ListMicrosoftTeamsChannelConfigurations",
        "chatbot:DescribeChimeWebhookConfigurations",
        "chatbot:DescribeSlackChannelConfigurations",
        "consoleapp:ListDeviceIdentities",
        "consoleapp:GetDeviceIdentity"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ServiceQuotasServiceRolePolicy

Beschreibung: Ermöglicht Service Quotas, in Ihrem Namen Supportanfragen zu erstellen

`ServiceQuotasServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 22. Mai 2019, 20:44 UTC
- Bearbeitete Zeit: 24. Juni 2019, 14:52 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/ServiceQuotasServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SignInLocalDevelopmentAccess

Beschreibung: Stellt Berechtigungen für den programmatischen Zugriff AWS über den AWS Anmeldedienst bereit, einschließlich der OAuth2 Token-Erstellung für Entwicklertools und -anwendungen.

`SignInLocalDevelopmentAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SignInLocalDevelopmentAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 19. November 2025, 18:34 UTC
- Bearbeitete Zeit: 19. November 2025, 18:34 UTC
- ARN: `arn:aws:iam::aws:policy/SignInLocalDevelopmentAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "signin:AuthorizeOAuth2Access",
        "signin:CreateOAuth2Token"
      ],
      "Resource" : "arn:aws:signin:*:*:oauth2/public-client/*"
```

```
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SimpleWorkflowFullAccess

Beschreibung: Bietet vollen Zugriff auf den Simple Workflow-Konfigurationsdienst.

`SimpleWorkflowFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SimpleWorkflowFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 6. Februar 2015, 18:41 UTC
- Zeit bearbeitet: 6. Februar 2015, 18:41 UTC
- ARN: `arn:aws:iam::aws:policy/SimpleWorkflowFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "swf:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SMSVoiceServiceRolePolicy

Beschreibung: Ermöglicht SMSVoice die Veröffentlichung von Metriken CloudWatch in Ihrem Namen

`SMSVoiceServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie

- Erstellungszeit: 14. November 2024, 17:04 UTC
- Bearbeitete Zeit: 14. November 2024, 17:04 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SMSVoiceServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : "cloudwatch:PutMetricData",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "cloudwatch:namespace" : "AWS/SMSVoice"
        }
      }
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SplitCostAllocationDataServiceRolePolicy

Beschreibung: Ermöglicht das Abrufen AWS von Unternehmensinformationen, falls zutreffend, und das Sammeln von Telemetriedaten für die Datendienste mit geteilter Kostenzuweisung, für die sich der Kunde entschieden hat.

`SplitCostAllocationDataServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 16. April 2024, 16:05 UTC
- Bearbeitete Zeit: 16. April 2024, 16:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SplitCostAllocationDataServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AwsOrganizationsAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListParents"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AmazonManagedServiceForPrometheusAccess",
      "Effect" : "Allow",
      "Action" : [
        "aps:ListWorkspaces",
        "aps:QueryMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SSMQuickSetupRolePolicy

Beschreibung: Stellt Berechtigungen bereit, um den Zustand der Quick Setup-Konfiguration zu überprüfen, die konsistente Verwendung von Parametern und bereitgestellten Ressourcen sicherzustellen und Ressourcen zu korrigieren, wenn Abweichungen festgestellt werden.

`SSMQuickSetupRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 25. Juni 2024, 15:20 Uhr UTC
- Bearbeitete Zeit: 18. November 2024, 13:06 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/SSMQuickSetupRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "SSMResourceDataSyncPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListResourceDataSync"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "SSMResourceDataSyncGetOpsSummaryPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:GetOpsSummary"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
    },
    {
      "Sid" : "SSMResourceDataSyncManagePermissions",
      "Effect" : "Allow",
```

```
      "Action" : [
        "ssm:DeleteResourceDataSync"
      ],
      "Resource" : "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*",
      "Condition" : {
        "StringEquals" : {
          "ssm:SyncType" : "SyncFromSource"
        }
      }
    },
    {
      "Sid" : "SSMAssociationsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListAssociations",
        "ssm:DescribeAssociationExecutions"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "QuickSetupSSMDocumentsReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "ssm:DescribeDocument",
        "ssm:GetDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
        "arn:aws:ssm:*:*:document/*-AWSQuickSetupType-*"
      ]
    },
    {
      "Sid" : "OrganizationReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListDelegatedServicesForAccount"
      ],
      "Resource" : "*"
```

```
    },
    {
      "Sid" : "QuickSetupStackSetReadOnlyPermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStackInstance",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:GetTemplate"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*"
      ]
    },
    {
      "Sid" : "QuickSetupStackSetDeletePermissions",
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet"
      ],
      "Resource" : [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:stackset-target/SSMQuickSetup*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ],
      "Condition" : {
        "StringEquals" : {
          "aws:ResourceAccount" : "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid" : "QuickSetupCfnStacksDescribePermissions",
```

```
      "Effect" : "Allow",
      "Action" : [
        "cloudformation:DescribeStacks",
        "cloudformation:ListStacks"
      ],
      "Resource" : [
        "*"
      ]
    }
  ]
}
```

Weitere Informationen

- Machen Sie sich mit der Versionierung für IAM-Richtlinien vertraut
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SupportUser

Beschreibung: Diese Richtlinie gewährt Berechtigungen zur Behebung und Lösung von Problemen in einem AWS-Konto. Diese Richtlinie ermöglicht es dem Benutzer auch, den AWS Support zu kontaktieren, um Fälle zu erstellen und zu verwalten.

`SupportUser`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SupportUser` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:21 Uhr UTC
- Bearbeitete Zeit: 10. Juli 2025, 17:07 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SupportUser`

Version der Richtlinie

Richtlinienversion: v9 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "support:*",
        "acm:DescribeCertificate",
        "acm:GetCertificate",
        "acm:List*",
        "acm-pca:DescribeCertificateAuthority",
        "acm-pca:ListCertificateAuthorities",
        "apigateway:GET",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "cloudformation:EstimateTemplateCost",
        "cloudfront:Get*",
        "cloudfront:List*",
        "cloudsearch:Describe*",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents",
        "cloudtrail:ListTags",
        "cloudtrail:ListPublicKeys",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codecommit:BatchGetRepositories",
        "codecommit:Get*",
```

```
        "codecommit:List*",
        "codedeploy:Batch*",
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:AcknowledgeJob",
        "codepipeline:AcknowledgeThirdPartyJob",
        "codepipeline:ListActionTypes",
        "codepipeline:ListPipelines",
        "codepipeline:PollForJobs",
        "codepipeline:PollForThirdPartyJobs",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipeline",
        "cognito-identity:List*",
        "cognito-identity:LookupDeveloperIdentity",
        "cognito-identity:Describe*",
        "cognito-idp:DescribeResourceServer",
        "cognito-idp:DescribeRiskConfiguration",
        "cognito-idp:DescribeUserImportJob",
        "cognito-idp:DescribeUserPool",
        "cognito-idp:DescribeUserPoolDomain",
        "cognito-idp:List*",
        "cognito-sync:Describe*",
        "cognito-sync:GetBulkPublishDetails",
        "cognito-sync:GetCognitoEvents",
        "cognito-sync:GetIdentityPoolConfiguration",
        "cognito-sync:List*",
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DescribeConfigRuleEvaluationStatus",
        "config:DescribeConfigRules",
        "config:DescribeDeliveryChannels",
        "config:DescribeDeliveryChannelStatus",
        "config:GetResourceConfigHistory",
        "config:ListDiscoveredResources",
        "datapipeline:DescribeObjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetPipelineDefinition",
        "datapipeline:ListPipelines",
        "datapipeline:QueryObjects",
        "datapipeline:ReportTaskProgress",
        "datapipeline:ReportTaskRunnerHeartbeat",
        "devicefarm:List*",
        "devicefarm:Get*",
        "directconnect:Describe*",
```

```
        "discovery:Describe*",
        "discovery:ListConfigurations",
        "dms:Describe*",
        "dms:List*",
        "ds:DescribeDirectories",
        "ds:DescribeSnapshots",
        "ds:GetDirectoryLimits",
        "ds:GetSnapshotLimits",
        "ds:ListAuthorizedApplications",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:ListTables",
        "ec2:Describe*",
        "ec2:DescribeHosts",
        "ec2:describeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeNatGateways",
        "ec2:DescribeReservedInstancesModifications",
        "ec2:DescribeTags",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:GetRepositoryPolicy",
        "ecr:BatchCheckLayerAvailability",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "elasticache:Describe*",
        "elasticache:List*",
        "elasticbeanstalk:Check*",
        "elasticbeanstalk:Describe*",
        "elasticbeanstalk:List*",
        "elasticbeanstalk:RequestEnvironmentInfo",
        "elasticbeanstalk:RetrieveEnvironmentInfo",
        "elasticbeanstalk:ValidateConfigurationSettings",
        "elasticfilesystem:Describe*",
        "elasticloadbalancing:Describe*",
        "elasticmapreduce:Describe*",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "elastictranscoder:ReadJob",
        "elasticfilesystem:DescribeFileSystems",
        "es:Describe*",
        "es:List*",
```

```
        "es:ESHttpGet",
        "es:ESHttpHead",
        "events:DescribeRule",
        "events:List*",
        "events:TestEventPattern",
        "firehose:Describe*",
        "firehose:List*",
        "gamelift:List*",
        "gamelift:Describe*",
        "glacier:ListVaults",
        "glacier:DescribeVault",
        "glacier:DescribeJob",
        "glacier:Get*",
        "glacier:List*",
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "importexport:GetStatus",
        "importexport:ListJobs",
        "inspector:Describe*",
        "inspector:List*",
        "iot:Describe*",
        "iot:Get*",
        "iot:List*",
        "kinesisanalytics:DescribeApplication",
        "kinesisanalytics:DiscoverInputSchema",
        "kinesisanalytics:GetApplicationState",
        "kinesisanalytics:ListApplications",
        "kinesis:Describe*",
        "kinesis:Get*",
        "kinesis:List*",
        "kms:Describe*",
        "kms:Get*",
        "kms:List*",
        "lambda:List*",
        "lambda:Get*",
        "logs:Describe*",
        "logs:TestMetricFilter",
        "machinelearning:Describe*",
        "machinelearning:Get*",
        "opsworks:Describe*",
        "rds:Describe*",
        "rds:ListTagsForResource",
```

```
        "redshift:Describe*",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
        "route53:Get*",
        "route53:List*",
        "route53domains:CheckDomainAvailability",
        "route53domains:GetDomainDetail",
        "route53domains:GetOperationDetail",
        "route53domains:List*",
        "s3:List*",
        "sdb:GetAttributes",
        "sdb:List*",
        "sdb:Select*",
        "servicecatalog:SearchProducts",
        "servicecatalog:DescribeProduct",
        "servicecatalog:DescribeProductView",
        "servicecatalog:ListLaunchPaths",
        "servicecatalog:DescribeProvisioningParameters",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:DescribeRecord",
        "servicecatalog:ScanProvisionedProducts",
        "ses:Get*",
        "ses:List*",
        "sns:Get*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "ssm:List*",
        "ssm:Describe*",
        "storagegateway:Describe*",
        "storagegateway:List*",
        "swf:Count*",
        "swf:Describe*",
        "swf:Get*",
        "swf:List*",
```

```
        "waf:Get*",
        "waf:List*",
        "workdocs:Describe*",
        "workmail:Describe*",
        "workmail:Get*",
        "workspaces:Describe*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

SystemAdministrator

Beschreibung: Gewährt vollständige Zugriffsberechtigungen, die für Ressourcen erforderlich sind, die für Anwendungs- und Entwicklungsvorgänge erforderlich sind.

`SystemAdministrator`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `SystemAdministrator` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:23 Uhr UTC
- Bearbeitete Zeit: 24. Juli 2025, 12:22 UTC
- ARN: `arn:aws:iam::aws:policy/job-function/SystemAdministrator`

Version der Richtlinie

Richtlinienversion: v8 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument


```
{
  "Statement" : [
    {
      "Action" : [
        "acm:Describe*",
        "acm:Get*",
        "acm:List*",
        "acm:Request*",
        "acm:Resend*",
        "autoscaling:*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:ListPublicKeys",
        "cloudtrail:ListTags",
        "cloudtrail:LookupEvents",
        "cloudtrail:StartLogging",
        "cloudtrail:StopLogging",
        "cloudwatch:*",
        "codecommit:BatchGetRepositories",
        "codecommit:CreateBranch",
        "codecommit:CreateRepository",
        "codecommit:Get*",
        "codecommit:GitPull",
        "codecommit:GitPush",
        "codecommit:List*",
        "codecommit:Put*",
        "codecommit:Test*",
        "codecommit:Update*",
        "codedeploy:*",
        "codepipeline:*",
        "config:*",
        "ds:*",
```

```
        "ec2:Allocate*",
        "ec2:AssignPrivateIpAddresses*",
        "ec2:Associate*",
        "ec2:Allocate*",
        "ec2:AttachInternetGateway",
        "ec2:AttachNetworkInterface",
        "ec2:AttachVpnGateway",
        "ec2:Bundle*",
        "ec2:Cancel*",
        "ec2:Copy*",
        "ec2:CreateCustomerGateway",
        "ec2:CreateDhcpOptions",
        "ec2:CreateFlowLogs",
        "ec2:CreateImage",
        "ec2:CreateInstanceExportTask",
        "ec2:CreateInternetGateway",
        "ec2:CreateKeyPair",
        "ec2:CreateLaunchTemplate",
        "ec2:CreateLaunchTemplateVersion",
        "ec2:CreateNatGateway",
        "ec2:CreateNetworkInterface",
        "ec2:CreatePlacementGroup",
        "ec2:CreateReservedInstancesListing",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateSpotDatafeedSubscription",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateVpc",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateVpnConnection",
        "ec2:CreateVpnConnectionRoute",
        "ec2:CreateVpnGateway",
        "ec2:DeleteFlowLogs",
        "ec2:DeleteKeyPair",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions",
        "ec2:DeleteNatGateway",
        "ec2:DeleteNetworkInterface",
        "ec2:DeletePlacementGroup",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DeleteSpotDatafeedSubscription",
        "ec2:DeleteSubnet",
        "ec2:DeleteTags",
        "ec2:DeleteVpc",
        "ec2:DeleteVpcEndpoints",
        "ec2:DeleteVpnConnection",
        "ec2:DeleteVpnConnectionRoute",
        "ec2:DeleteVpnGateway",
        "ec2:DeregisterImage",
        "ec2:Describe*",
        "ec2:DetachInternetGateway",
        "ec2:DetachNetworkInterface",
        "ec2:DetachVpnGateway",
        "ec2:DisableVgwRoutePropagation",
        "ec2:DisableVpcClassicLinkDnsSupport",
        "ec2:DisassociateAddress",
        "ec2:DisassociateRouteTable",
        "ec2:EnableVgwRoutePropagation",
        "ec2:EnableVolumeIO",
        "ec2:EnableVpcClassicLinkDnsSupport",
        "ec2:GetConsoleOutput",
        "ec2:GetHostReservationPurchasePreview",
        "ec2:GetLaunchTemplateData",
        "ec2:GetPasswordData",
        "ec2:GetSecurityGroupsForVpc",
        "ec2:Import*",
        "ec2:Modify*",
        "ec2:MonitorInstances",
        "ec2:MoveAddressToVpc",
        "ec2:Purchase*",
        "ec2:RegisterImage",
        "ec2:Release*",
        "ec2:Replace*",
        "ec2:ReportInstanceStatus",
        "ec2:Request*",
        "ec2:Reset*",
        "ec2:RestoreAddressToClassic",
        "ec2:RunScheduledInstances",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:UnmonitorInstances",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "elasticloadbalancing:*",
        "events:*",
```

```
        "iam:GetAccount*",
        "iam:GetContextKeys*",
        "iam:GetCredentialReport",
        "iam:ListAccountAliases",
        "iam:ListGroups",
        "iam:ListOpenIDConnectProviders",
        "iam:ListPolicies",
        "iam:ListPoliciesGrantingServiceAccess",
        "iam:ListRoles",
        "iam:ListSAMLProviders",
        "iam:ListServerCertificates",
        "iam:Simulate*",
        "iam:UpdateServerCertificate",
        "iam:UpdateSigningCertificate",
        "kinesis:ListStreams",
        "kinesis:PutRecord",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:Describe*",
        "kms:GenerateRandom",
        "kms:Get*",
        "kms:List*",
        "kms:Encrypt",
        "kms:ReEncrypt*",
        "lambda:Create*",
        "lambda:Delete*",
        "lambda:Get*",
        "lambda:InvokeFunction",
        "lambda:List*",
        "lambda:PublishVersion",
        "lambda:Update*",
        "logs:*",
        "rds:Describe*",
        "rds:ListTagsForResource",
        "rolesanywhere:GetCrl",
        "rolesanywhere:GetProfile",
        "rolesanywhere:GetSubject",
        "rolesanywhere:GetTrustAnchor",
        "rolesanywhere:ListCrls",
        "rolesanywhere:ListProfiles",
        "rolesanywhere:ListSubjects",
        "rolesanywhere:ListTagsForResource",
        "rolesanywhere:ListTrustAnchors",
```

```
        "rolesanywhere:PutNotificationSettings",
        "rolesanywhere:ResetNotificationSettings",
        "route53:*",
        "route53domains:*",
        "ses:*",
        "sns:*",
        "sqs:*",
        "trustedadvisor:*"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    },
    {
      "Action" : [
        "ec2:AcceptVpcPeeringConnection",
        "ec2:AttachClassicLinkVpc",
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateVpcPeeringConnection",
        "ec2:DeleteCustomerGateway",
        "ec2:DeleteDhcpOptions",
        "ec2:DeleteInternetGateway",
        "ec2:DeleteNetworkAcl*",
        "ec2:DeleteRoute",
        "ec2:DeleteRouteTable",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteVolume",
        "ec2:DeleteVpcPeeringConnection",
        "ec2:DetachClassicLinkVpc",
        "ec2:DetachVolume",
        "ec2:DisableVpcClassicLink",
        "ec2:EnableVpcClassicLink",
        "ec2:GetConsoleScreenshot",
        "ec2:RebootInstances",
        "ec2:RejectVpcPeeringConnection",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Effect" : "Allow",
```

```
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : "s3:*",
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
    {
      "Action" : [
        "iam:GetAccessKeyLastUsed",
        "iam:GetGroup*",
        "iam:GetInstanceProfile",
        "iam:GetLoginProfile",
        "iam:GetOpenIDConnectProvider",
        "iam:GetPolicy*",
        "iam:GetRole*",
        "iam:GetSAMLProvider",
        "iam:GetSSHPublicKey",
        "iam:GetServerCertificate",
        "iam:GetServiceLastAccessed*",
        "iam:GetUser*",
        "iam:ListAccessKeys",
        "iam:ListAttached*",
        "iam:ListEntitiesForPolicy",
        "iam:ListGroupPolicies",
        "iam:ListGroupsForUser",
        "iam:ListInstanceProfiles*",
        "iam:ListMFADevices",
        "iam:ListPolicyVersions",
        "iam:ListRolePolicies",
        "iam:ListSSHPublicKeys",
        "iam:ListSigningCertificates",
        "iam:ListUserPolicies",
        "iam:Upload*"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "*"
      ]
    },
```

```
    {
      "Action" : [
        "iam:GetRole",
        "iam:ListRoles",
        "iam:PassRole"
      ],
      "Effect" : "Allow",
      "Resource" : [
        "arn:aws:iam::*:role/rds-monitoring-role",
        "arn:aws:iam::*:role/ec2-sysadmin-*",
        "arn:aws:iam::*:role/ecr-sysadmin-*",
        "arn:aws:iam::*:role/lambda-sysadmin-*"
      ]
    }
  ],
  "Version" : "2012-10-17"
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

TranslateFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon Translate.

`TranslateFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `TranslateFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 27. November 2018, 23:36 UTC

- Bearbeitete Zeit: 8. Januar 2020, 21:22 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Action" : [
        "translate:*",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Effect" : "Allow",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

TranslateReadOnly

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon Translate.

`TranslateReadOnly`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `TranslateReadOnly` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2017, 18:22 UTC
- Bearbeitete Zeit: 24. Mai 2023, 17:19 UTC
- ARN: `arn:aws:iam::aws:policy/TranslateReadOnly`

Version der Richtlinie

Richtlinienversion: v7 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "translate:TranslateText",
        "translate:TranslateDocument",
```

```
        "translate:GetTerminology",
        "translate:ListTerminologies",
        "translate:ListTextTranslationJobs",
        "translate:DescribeTextTranslationJob",
        "translate:GetParallelData",
        "translate:ListParallelData",
        "comprehend:DetectDominantLanguage",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

ViewOnlyAccess

Beschreibung: Diese Richtlinie gewährt Berechtigungen zum Anzeigen von Ressourcen und grundlegenden Metadaten für alle AWS Dienste.

`ViewOnlyAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `ViewOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Art: Richtlinie für Job Funktionen
- Erstellungszeit: 10. November 2016, 17:20 Uhr UTC
- Bearbeitete Zeit: 13. Oktober 2025, 21:34 UTC

- ARN: `arn:aws:iam::aws:policy/job-function/ViewOnlyAccess`

Version der Richtlinie

Richtlinienversion: v27 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "GeneralViewOnlyAccessStatement",
      "Effect" : "Allow",
      "Action" : [
        "acm:ListCertificates",
        "aiops:GetInvestigation",
        "aiops:GetInvestigationGroup",
        "aiops:ListInvestigationEvents",
        "aiops:ListInvestigationGroups",
        "aiops:ListInvestigations",
        "athena:List*",
        "autoscaling:Describe*",
        "aws-marketplace:ViewSubscriptions",
        "backup:DescribeBackupJob",
        "backup:DescribeBackupVault",
        "backup:DescribeCopyJob",
        "backup:DescribeFramework",
        "backup:DescribeGlobalSettings",
        "backup:DescribeProtectedResource",
        "backup:DescribeRecoveryPoint",
        "backup:DescribeRegionSettings",
        "backup:DescribeReportJob",
        "backup:DescribeReportPlan",
        "backup:DescribeRestoreJob",
        "backup:GetSupportedResourceTypes",
        "backup:ListBackupJobs",
```

```
        "backup:ListBackupPlans",
        "backup:ListBackupPlanTemplates",
        "backup:ListBackupPlanVersions",
        "backup:ListBackupSelections",
        "backup:ListBackupVaults",
        "backup:ListCopyJobs",
        "backup:ListFrameworks",
        "backup:ListLegalHolds",
        "backup:ListProtectedResources",
        "backup:ListProtectedResourcesByBackupVault",
        "backup:ListRecoveryPointsByBackupVault",
        "backup:ListRecoveryPointsByLegalHold",
        "backup:ListRecoveryPointsByResource",
        "backup:ListReportJobs",
        "backup:ListReportPlans",
        "backup:ListRestoreJobs",
        "backup:ListTags",
        "batch:ListJobs",
        "bedrock:ListCustomModels",
        "bedrock:ListTagsForResource",
        "clouddirectory:ListAppliedSchemaArns",
        "clouddirectory:ListDevelopmentSchemaArns",
        "clouddirectory:ListDirectories",
        "clouddirectory:ListPublishedSchemaArns",
        "cloudformation:DescribeStacks",
        "cloudformation:List*",
        "cloudfront:List*",
        "cloudsearch:DescribeDomains",
        "cloudsearch:List*",
        "cloudtrail:DescribeTrails",
        "cloudtrail:ListTrails",
        "cloudtrail:LookupEvents",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "codebuild:ListBuilds*",
        "codebuild:ListProjects",
        "codecommit:List*",
        "codedeploy:BatchGetApplicationRevisions",
        "codedeploy:BatchGetApplications",
        "codedeploy:BatchGetDeploymentGroups",
        "codedeploy:BatchGetDeploymentInstances",
        "codedeploy:BatchGetDeployments",
        "codedeploy:BatchGetDeploymentTargets",
        "codedeploy:BatchGetOnPremisesInstances",
```

```
        "codedeploy:Get*",
        "codedeploy:List*",
        "codepipeline:ListPipelines",
        "codestar:List*",
        "cognito-identity:ListIdentities",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:List*",
        "cognito-sync:ListDatasets",
        "comprehend:Describe*",
        "comprehend:List*",
        "config:Describe*",
        "config:List*",
        "connect:List*",
        "cost-optimization-hub:GetPreferences",
        "cost-optimization-hub:GetRecommendation",
        "cost-optimization-hub:ListEnrollmentStatuses",
        "cost-optimization-hub:ListRecommendations",
        "cost-optimization-hub:ListRecommendationSummaries",
        "databrew:ListJobs",
        "databrew:ListProjects",
        "datapipeline:DescribePipelines",
        "datapipeline:GetAccountLimits",
        "datapipeline:ListPipelines",
        "dax:DescribeClusters",
        "dax:DescribeDefaultParameters",
        "dax:DescribeEvents",
        "dax:DescribeParameterGroups",
        "dax:DescribeParameters",
        "dax:DescribeSubnetGroups",
        "dax:ListTags",
        "devicefarm:List*",
        "directconnect:Describe*",
        "discovery:List*",
        "dms:List*",
        "ds:DescribeDirectories",
        "dynamodb:DescribeBackup",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeGlobalTable",
        "dynamodb:DescribeGlobalTableSettings",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeReservedCapacity",
        "dynamodb:DescribeReservedCapacityOfferings",
        "dynamodb:DescribeStream",
        "dynamodb:DescribeTable",
```

```
        "dynamodb:DescribeTimeToLive",
        "dynamodb:ListBackups",
        "dynamodb:ListExports",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListStreams",
        "dynamodb:ListTables",
        "dynamodb:ListTagsOfResource",
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeBundleTasks",
        "ec2:DescribeCarrierGateways",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeConversionTasks",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeExportTasks",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeHost*",
        "ec2:DescribeIdentityIdFormat",
        "ec2:DescribeIdFormat",
        "ec2:DescribeImage*",
        "ec2:DescribeImport*",
        "ec2:DescribeInstance*",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeLocalGatewayRouteTables",
        "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations",
        "ec2:DescribeLocalGateways",
        "ec2:DescribeLocalGatewayVirtualInterfaceGroups",
        "ec2:DescribeLocalGatewayVirtualInterfaces",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetwork*",
        "ec2:DescribePlacementGroups",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRegions",
        "ec2:DescribeReserved*",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshot*",
        "ec2:DescribeSpot*",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolume*",
        "ec2:DescribeVpc*",
        "ec2:DescribeVpnGateways",
        "ec2:SearchLocalGatewayRoutes",
        "ecr:DescribeRegistry",
        "ecr:DescribeRepositories",
        "ecr:ListImages",
        "ecs:Describe*",
        "ecs:List*",
        "eks:ListTagsForResource",
        "elasticache:Describe*",
        "elasticbeanstalk:DescribeApplications",
        "elasticbeanstalk:DescribeApplicationVersions",
        "elasticbeanstalk:DescribeEnvironments",
        "elasticbeanstalk:ListAvailableSolutionStacks",
        "elasticfilesystem:DescribeFileSystems",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeListeners",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticmapreduce:List*",
        "elastictranscoder:List*",
        "emr-serverless:ListApplications",
        "es:DescribeElasticsearchDomain",
        "es:DescribeElasticsearchDomains",
        "es:ListDomainNames",
        "events:ListRuleNamesByTarget",
        "events:ListRules",
        "events:ListTargetsByRule",
        "firehose:DescribeDeliveryStream",
        "firehose:List*",
        "fsx:DescribeFileSystems",
        "gamelift:List*",
        "glacier:List*",
        "glue:GetTags",
        "greengrass:List*",
        "iam:GetAccountSummary",
        "iam:GetLoginProfile",
        "iam:List*",
        "importexport:ListJobs",
```

```
        "inspector:List*",
        "iot:List*",
        "kafka:ListClusters",
        "kendra:ListDataSources",
        "kendra:ListTagsForResource",
        "kinesis:ListStreams",
        "kinesisanalytics:ListApplications",
        "kinesisanalytics:ListTagsForResource",
        "kms:ListKeys",
        "kms:ListResourceTags",
        "lambda:List*",
        "lex:GetBotAliases",
        "lex:GetBotChannelAssociations",
        "lex:GetBots",
        "lex:GetBotVersions",
        "lex:GetIntents",
        "lex:GetIntentVersions",
        "lex:GetSlotTypes",
        "lex:GetSlotTypeVersions",
        "lex:GetUtterancesView",
        "lightsail:GetBlueprints",
        "lightsail:GetBundles",
        "lightsail:GetInstances",
        "lightsail:GetInstanceSnapshots",
        "lightsail:GetKeyPair",
        "lightsail:GetRegions",
        "lightsail:GetStaticIps",
        "lightsail:IsVpcPeered",
        "logs:Describe*",
        "logs:GetTransformer",
        "logs:ListEntitiesForLogGroup",
        "logs:ListLogGroupsForEntity",
        "logs:ListLogGroupsForQuery",
        "logs:ListTagsForResource",
        "lookoutvision:ListModelPackagingJobs",
        "lookoutvision:ListModels",
        "lookoutvision:ListProjects",
        "m2:GetApplication",
        "m2:GetEnvironment",
        "m2:ListApplications",
        "m2:ListEnvironments",
        "m2:ListTagsForResource",
        "machinelearning:Describe*",
        "mediaconnect:ListEntitlements",
```

```
            "mediaconnect:ListFlows",
            "mediaconnect:ListOfferings",
            "mediaconnect:ListReservations",
            "mobiletargeting:GetApplicationSettings",
            "mobiletargeting:GetCampaigns",
            "mobiletargeting:GetImportJobs",
            "mobiletargeting:GetSegments",
            "oam:ListAttachedLinks",
            "oam:ListLinks",
            "oam:ListSinks",
            "opsworks-cm:Describe*",
            "opsworks:Describe*",
            "organizations:List*",
            "outposts:GetOutpost",
            "outposts:GetOutpostInstanceTypes",
            "outposts:ListOutposts",
            "outposts:ListSites",
            "outposts:ListTagsForResource",
            "polly:Describe*",
            "polly:List*",
            "profile:ListDomains",
            "profile:ListIntegrations",
            "rds:Describe*",
            "redshift-serverless:ListTagsForResource",
            "redshift-serverless:ListWorkgroups",
            "redshift:DescribeClusters",
            "redshift:DescribeEvents",
            "redshift:ViewQueriesInConsole",
            "resource-explorer-2:GetDefaultView",
            "resource-explorer-2:GetIndex",
            "resource-explorer-2:ListIndexes",
            "resource-explorer-2:ListSupportedResourceTypes",
            "resource-explorer-2:ListTagsForResource",
            "resource-explorer-2:ListViews",
            "rolesanywhere:ListCrls",
            "rolesanywhere:ListProfiles",
            "rolesanywhere:ListSubjects",
            "rolesanywhere:ListTagsForResource",
            "rolesanywhere:ListTrustAnchors",
            "route53:Get*",
            "route53:List*",
            "route53domains:List*",
            "route53profiles:GetProfile",
            "route53profiles:GetProfileAssociation",
```

```
        "route53profiles:GetProfileResourceAssociation",
        "route53profiles:ListProfileAssociations",
        "route53profiles:ListProfileResourceAssociations",
        "route53profiles:ListProfiles",
        "route53profiles:ListTagsForResource",
        "route53resolver:Get*",
        "route53resolver:List*",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListMultiRegionAccessPoints",
        "sagemaker:Describe*",
        "sagemaker:List*",
        "sdb:List*",
        "servicecatalog:List*",
        "ses:DescribeActiveReceiptRuleSet",
        "ses:List*",
        "ses:ListDedicatedIpPools",
        "shield:List*",
        "sns:List*",
        "sqs:GetQueueAttributes",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ListMessageMoveTasks",
        "sqs:ListQueues",
        "sqs:ListQueueTags",
        "ssm:ListAssociations",
        "ssm:ListDocuments",
        "states:ListActivities",
        "states:ListExecutions",
        "states:ListMapRuns",
        "states:ListStateMachineAliases",
        "states:ListStateMachines",
        "states:ListStateMachineVersions",
        "storagegateway:ListGateways",
        "storagegateway:ListLocalDisks",
        "storagegateway:ListVolumeRecoveryPoints",
        "storagegateway:ListVolumes",
        "swf:List*",
        "trustedadvisor:Describe*",
        "waf-regional:List*",
        "waf:List*",
        "wafv2:List*",
        "workdocs:DescribeAvailableDirectories",
        "workdocs:DescribeInstances",
```

```
        "workmail:Describe*",
        "workspaces:Describe*"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Sid" : "APIGatewayAccess",
      "Action" : [
        "apigateway:GET"
      ],
      "Resource" : [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers/*",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/cors",
        "arn:aws:apigateway:*::/apis/*/deployments/*",
        "arn:aws:apigateway:*::/apis/*/deployments",
        "arn:aws:apigateway:*::/apis/*/exports/*",
        "arn:aws:apigateway:*::/apis/*/integrations/*",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/models/*",
        "arn:aws:apigateway:*::/apis/*/models",
        "arn:aws:apigateway:*::/apis/*/routes/*",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/apis/*/stages",
        "arn:aws:apigateway:*::/apis/*/stages/*",
        "arn:aws:apigateway:*::/clientcertificates",
        "arn:aws:apigateway:*::/clientcertificates/*",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/apimappings",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers/*",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/deployments/*",
        "arn:aws:apigateway:*::/restapis/*/deployments",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/parts",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions/*",
        "arn:aws:apigateway:*::/restapis/*/documentation/versions",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses/*",
        "arn:aws:apigateway:*::/restapis/*/gatewayresponses",
        "arn:aws:apigateway:*::/restapis/*/models/*",
        "arn:aws:apigateway:*::/restapis/*/models",
```

```
        "arn:aws:apigateway:*::/restapis/*/requestvalidators",
        "arn:aws:apigateway:*::/restapis/*/requestvalidators/*",
        "arn:aws:apigateway:*::/restapis/*/resources/*",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages",
        "arn:aws:apigateway:*::/restapis/*/stages/*",
        "arn:aws:apigateway:*::/tags/*",
        "arn:aws:apigateway:*::/vpclinks"
      ]
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VMImportExportRoleForAWSConnector

Beschreibung: Standardrichtlinie für die Import/Export VM-Dienstrolle für Kunden, die den AWS Connector verwenden. Der Import/Export VM-Dienst übernimmt mit dieser Richtlinie eine Rolle bei der Erfüllung von Migrationsanfragen für virtuelle Maschinen von der virtuellen AWS Connector-Appliance. (Beachten Sie, dass der AWS Connector die verwaltete Richtlinie AWSConnector "" verwendet, um Anfragen im Namen des Kunden an den Import/Export VM-Dienst zu richten.) Bietet die Möglichkeit, EBS-Snapshots zu erstellen AMIs , EBS-Snapshot-Attribute zu ändern, „Describe*“ -Aufrufe für EC2 Objekte durchzuführen und aus S3-Buckets zu lesen, die mit '2' beginnen. import-to-ec

`VMImportExportRoleForAWSConnector`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `VMImportExportRoleForAWSConnector` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: Richtlinie für Servicerollen
- Erstellungszeit: 3. September 2015, 20:48 UTC
- Bearbeitete Zeit: 3. September 2015, 20:48 UTC
- ARN: `arn:aws:iam::aws:policy/service-role/VMImportExportRoleForAWSConnector`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject"
      ],
      "Resource" : [
        "arn:aws:s3:::import-to-ec2-*"
      ]
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeFullAccess

Beschreibung: Bietet vollen Zugriff auf Amazon VPC Lattice und Zugriff auf Abhängigkeitsdienste.

`VPCLatticeFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `VPCLatticeFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:49 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeFullAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS

Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "logs:DescribeLogGroups",
        "s3:ListAllMyBuckets",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:UpdateLogDelivery",
```

```
        "logs:DescribeResourcePolicies"
      ],
      "Resource" : "*",
      "Condition" : {
        "ForAnyValue:StringEquals" : {
          "aws:CalledVia" : [
            "vpc-lattice.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "vpc-lattice.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/delivery.logs.amazonaws.com/
AWSServiceRoleForLogDelivery",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "delivery.logs.amazonaws.com"
        }
      }
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
      ],
      "Resource" : "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice"
    }
  ]
```

```
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf Amazon VPC Lattice über die und eingeschränkten Zugriff auf AWS-Managementkonsole Abhängigkeitsdienste.

`VPCLatticeReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `VPCLatticeReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:47 UTC
- Bearbeitete Zeit: 1. Dezember 2024, 14:21 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice:Get*",
        "vpc-lattice:List*",
        "acm:DescribeCertificate",
        "acm:ListCertificates",
        "cloudwatch:GetMetricData",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcs",
        "elasticloadbalancing:DescribeLoadBalancers",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "lambda:ListAliases",
        "lambda:ListFunctions",
        "lambda:ListVersionsByFunction",
        "logs:DescribeLogGroups",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "s3:ListAllMyBuckets",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

VPCLatticeServicesInvokeAccess

Beschreibung: Ermöglicht den Zugriff auf das Aufrufen von Amazon VPC Lattice-Diensten.

`VPCLatticeServicesInvokeAccess`ist eine verwaltete Richtlinie AWS .

Diese Richtlinie wird verwendet

Sie können `VPCLatticeServicesInvokeAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 30. März 2023, 02:45 UTC
- Bearbeitete Zeit: 30. März 2023, 02:45 UTC
- ARN: `arn:aws:iam::aws:policy/VPCLatticeServicesInvokeAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "vpc-lattice-svcs:Invoke"
```

```
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFLoggingServiceRolePolicy

Beschreibung: SLR erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

`WAFLoggingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2018, 21:05 Uhr UTC
- Bearbeitete Zeit: 24. August 2018, 21:05 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFLoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFRegionalLoggingServiceRolePolicy

Beschreibung: SLR erstellen, um Kundenprotokolle in einen Firehose-Stream zu schreiben

`WAFRegionalLoggingServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 24. August 2018, 18:40 Uhr UTC
- Bearbeitete Zeit: 24. August 2018, 18:40 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFRegionalLoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WAFV2LoggingServiceRolePolicy

Beschreibung: Diese Richtlinie erstellt eine serviceverknüpfte Rolle, die es AWS WAF ermöglicht, Protokolle in Amazon Kinesis Data Firehose zu schreiben.

`WAFV2LoggingServiceRolePolicy`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es dem Dienst ermöglicht, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht an Ihre Benutzer, Gruppen oder Rollen anhängen.

Einzelheiten der Richtlinie

- Typ: Dienstbezogene Rollenrichtlinie
- Erstellungszeit: 7. November 2019, 00:40 UTC
- Bearbeitete Zeit: 03. Juni 2024, 17:29 UTC
- ARN: `arn:aws:iam::aws:policy/aws-service-role/WAFV2LoggingServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v3 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
```

```
    {
      "Sid" : "FirehoseAPIStatement",
      "Effect" : "Allow",
      "Action" : [
        "firehose:PutRecord",
        "firehose:PutRecordBatch"
      ],
      "Resource" : [
        "arn:aws:firehose:*:*:deliverystream/aws-waf-logs-*"
      ]
    },
    {
      "Sid" : "DescribeOrganizationAPIStatement",
      "Effect" : "Allow",
      "Action" : "organizations:DescribeOrganization",
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Verstehen Sie die Versionierung für IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WellArchitectedConsoleFullAccess

Beschreibung: Bietet vollen Zugriff auf das AWS Well-Architected Tool über das AWS-Managementkonsole

`WellArchitectedConsoleFullAccess`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `WellArchitectedConsoleFullAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie

- Erstellungszeit: 29. November 2018, 18:19 Uhr UTC
- Zeit bearbeitet: 29. November 2018, 18:19 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleFullAccess`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:*"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WellArchitectedConsoleReadOnlyAccess

Beschreibung: Bietet schreibgeschützten Zugriff auf das AWS Well-Architected Tool über AWS-Managementkonsole

`WellArchitectedConsoleReadOnlyAccess`ist eine verwaltete Richtlinie.AWS

Diese Richtlinie wird verwendet

Sie können `WellArchitectedConsoleReadOnlyAccess` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 29. November 2018, 18:21 Uhr UTC
- Bearbeitete Zeit: 29. Juni 2023, 17:16 UTC
- ARN: `arn:aws:iam::aws:policy/WellArchitectedConsoleReadOnlyAccess`

Version der Richtlinie

Richtlinienversion: v2 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "wellarchitected:Get*",
        "wellarchitected:List*",
```

```
        "wellarchitected:ExportLens"
      ],
      "Resource" : "*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

WorkLinkServiceRolePolicy

Beschreibung: Ermöglicht den Zugriff auf AWS-Services und Ressourcen, die von Amazon verwendet oder verwaltet werden WorkLink

`WorkLinkServiceRolePolicy`ist eine AWS verwaltete Richtlinie.

Diese Richtlinie wird verwendet

Sie können `WorkLinkServiceRolePolicy` an Ihre Benutzer, Gruppen und Rollen anfügen.

Einzelheiten zur Richtlinie

- Typ: AWS verwaltete Richtlinie
- Erstellungszeit: 23. Januar 2019, 19:03 UTC
- Bearbeitete Zeit: 23. Januar 2019, 19:03 UTC
- ARN: `arn:aws:iam::aws:policy/WorkLinkServiceRolePolicy`

Version der Richtlinie

Richtlinienversion: v1 (Standard)

Die Standardversion der Richtlinie ist die Version, die die Berechtigungen für die Richtlinie definiert. Wenn ein Benutzer oder eine Rolle mit der Richtlinie eine Anfrage zum Zugriff auf eine AWS Ressource stellt, AWS überprüft er die Standardversion der Richtlinie, um festzustellen, ob die Anfrage zulässig ist.

JSON-Richtliniendokument

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource" : "*"
    },
    {
      "Effect" : "Allow",
      "Action" : [
        "kinesis:PutRecord",
        "kinesis:PutRecords"
      ],
      "Resource" : "arn:aws:kinesis:*:*:stream/AmazonWorkLink-*"
    }
  ]
}
```

Weitere Informationen

- Erstellen Sie einen Berechtigungssatz mithilfe AWS verwalteter Richtlinien im IAM Identity Center
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Verstehen Sie die Versionierung von IAM-Richtlinien
- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.